TERRORISM

COMMENTARY ON SECURITY DOCUMENTS

VOLUME
141

HYBRID WARFARE AND THE GRAY ZONE THREAT

EDITED BY
DOUGLAS C. LOVELACE, JR.

OXFORD

TERRORISM

Commentary on Security Documents

VOLUME 141

TERRORISM

Commentary on Security Documents

VOLUME 141

HYBRID WARFARE AND THE GRAY ZONE THREAT

Douglas C. Lovelace, Jr.
Senior National Security Strategist

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Oxford University Press is a department of the University of Oxford. It furthers the University's objective of excellence in research, scholarship, and education by publishing worldwide.

Oxford New York
Auckland Cape Town Dar es Salaam Hong Kong Karachi
Kuala Lumpur Madrid Melbourne Mexico City Nairobi
New Delhi Shanghai Taipei Toronto

With offices in
Argentina Austria Brazil Chile Czech Republic France Greece
Guatemala Hungary Italy Japan Poland Portugal Singapore
South Korea Switzerland Thailand Turkey Ukraine Vietnam

Oxford is a registered trademark of Oxford University Press in the UK and certain other countries.

Published in the United States of America by
Oxford University Press
198 Madison Avenue, New York, NY 10016

Copyright © 2016 by Oxford University Press

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior permission in writing of Oxford University Press, or as expressly permitted by law, by license, or under terms agreed with the appropriate reproduction rights organization. Inquiries concerning reproduction outside the scope of the above should be sent to the Rights Department, Oxford University Press, at the address above.

You must not circulate this work in any other form
and you must impose this same condition on any acquirer.

Cataloging-in-Publication information is available from the Library of Congress.

ISSN 1062-4007
Terrorism: Commentary on Security Documents

ISBN 978-0-19-025531-2 (v. 141)

Printed in the United States of America on acid-free paper

Note to Readers

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is based upon sources believed to be accurate and reliable and is intended to be current as of the time it was written. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. Also, to confirm that the information has not been affected or changed by recent developments, traditional legal research techniques should be used, including checking primary sources where appropriate.

(Based on the Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers and Associations.)

You may order this or any other Oxford University Press publication
by visiting the Oxford University Press website at www.oup.com

TABLE OF CONTENTS

VOLUME 141

HYBRID WARFARE AND THE GRAY ZONE THREAT

Preface ix

DOCUMENTS

A. THE SHIFTING INTERNATIONAL SECURITY ENVIRONMENT

Commentary by Douglas C. Lovelace, Jr. 3

DOCUMENT NO. 1*: A Shift in the International Security Environment: Potential Implications for Defense—Issues for Congress*, CRS Report No. R43838, Ronald O'Rourke, July 14, 2015. 5

B. UNDERSTANDING HYBRID WARFARE AND GRAY ZONE THREATS

Commentary by Douglas C. Lovelace, Jr. 49

DOCUMENT NO. 2: *Hybrid Warfare,* Timothy B. McCulloh and Richard Johnson, Joint Special Operations University, MacDill Air Force Base, FL, August 2013 53

DOCUMENT NO. 3: *Hybrid Warfare,* Davi M. D'Agostino, Government Accountability Office Report to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, Washington, D.C., September 10, 2010 145

DOCUMENT NO. 4: *SOF Support to Political Warfare*, White Paper, United States Army Special Operations Command, March 10, 2015 159

C. CYBERSECURITY AND OPERATIONS

Commentary by Douglas C. Lovelace, Jr. 201

DOCUMENT NO. 5: *Cyber Operations in DOD Policy and Plans: Issues for Congress*, CRS Report No. R43848, Catherine A. Theohary and Anne I. Harrington, January 5, 2015 203

DOCUMENT NO. 6: *CYBERSECURITY: Actions Needed to Address Challenges Facing Federal Systems*, Testimony Before the Committee on Oversight and Government Reform, House of Representatives, Statement of Gregory C. Wilshusen, Government Accountability Office, Washington, D.C., April 22, 2015 237

DOCUMENT NO. 7: *CYBERSECURITY: Recent Data Breaches Illustrate Need for Strong Controls Across Federal Agencies*, Testimony Before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives, Statement of Gregory C. Wilshusen, Government Accountability Office, Washington, D.C., June 24, 2015 251

DOCUMENT NO. 8: *Cyberwarfare and Cyberterrorism: In Brief*, CRS Report No. R43955, Catherine A. Theohary and John W. Rollins, March 27, 2015 263

D. THE EFFICACY OF SANCTIONS IN AVOIDING HYBRID WARFARE AND DETERRING GRAY ZONE THREATS

Commentary by Douglas C. Lovelace, Jr. 279

DOCUMENT NO. 9: *NONPROLIFERATION: State Should Minimize Reporting Delays That May Affect Sanctions on Trade with Iran, North Korea, and Syria*, Report to the Chairman, Committee on Foreign Affairs, House of Representatives, Government Accountability Office, Washington, D.C., May 2015 281

DOCUMENT NO. 10: *NORTH KOREA SANCTIONS: United States Has Increased Flexibility to Impose Sanctions, but United Nations Is Impeded by a Lack of Member State Reports*, Report to the Chairman, Committee on Foreign Relations, U.S. Senate, Government Accountability Office, Washington, D.C., May 2015 305

E. THE MILITARY AND LAW ENFORCEMENT

Commentary by Douglas C. Lovelace, Jr. 347

DOCUMENT NO. 11: *CIVIL SUPPORT: DOD Is Taking Action to Strengthen Support of Civil Authorities*, Testimony Before the Subcommittee on Emergency Preparedness, Response, and Communications, Committee on Homeland Security, House of Representatives, Statement of Joseph W. Kirschbaum, Ph.D., Government Accountability Office, Washington, D.C., June 10, 2015 349

DOCUMENT NO. 12: *The "1033 Program," Department of Defense Support to Law Enforcement*, CRS Report No. R43701, Daniel H. Else, August 28, 2014 361

DOCUMENT NO. 13: *The "Militarization" of Law Enforcement and the Department of Defense's "1033 Program,"* Nathan James and Daniel H. Else, CRS Insights, December 2, 2014 367

SUBJECT INDEX 371

PREFACE

by
Douglas C. Lovelace, Jr.

Hybrid warfare is a commonly used term that is not defined formally within the U.S. Department of Defense (DOD) and military lexicon. Nonetheless, it provides a useful shorthand expression for the mutation of the international security environment brought on by decades of unrivaled U.S. conventional military power. It encompasses conventional warfare, irregular warfare, cyberwarfare, insurgency, criminality, economic blackmail, ethnic warfare, "lawfare," and the application of low-cost but effective technologies to thwart high-cost technologically advanced forces. Hybrid warfare targets entire societies, not just nations' military forces. In many cases, aggressors employ elements of hybrid warfare either in measures just under their adversaries' thresholds for response or in ways that make attribution too uncertain to justify lethal responses—this area is sometimes called the "Gray Zone." In most cases, hybrid adversaries prefer to achieve their aims without resort to politically and economically costly traditional warfare.

Many national security strategists view hybrid warfare and Gray Zone threats to be the most perplexing features of the evolving international security environment, in that dealing with them requires highly versatile, adaptable, and scalable military forces. While the United States and other major powers have been attempting to convert Cold War legacy forces to those more appropriate for the international security environment of today and tomorrow, such efforts have been largely hidebound.

This volume presents thirteen documents divided into five sections to help readers better understand the nature of hybrid warfare and Gray Zone threats. To set the context, Section A presents the Congressional Research Service (CRS) report, *A Shift in the International Security Environment: Potential Implications for Defense—Issues for Congress.* Section B, "Understanding Hybrid Warfare and Gray Zone Threats," informs readers of the many aspects of such conflicts and belligerents first by presenting the comprehensive Joint Special Operations University's report on *Hybrid Warfare*. Armed with in-depth understanding of the phenomenon, readers are then presented with a Government Accountability Office (GAO) report also entitled *Hybrid Warfare*. We complete Section B with a United States Army Special Operations Command report on *SOF (Special Operations Forces) Support to Political Warfare*.

Section C, "Cybersecurity and Operations," contains four documents that address cyberwarfare from several perspectives: a CRS Report on *Cyber Operations in DOD Policy and Plans: Issues for Congress*; a GAO report on *Cybersecurity: Actions Needed to*

Address Challenges Facing Federal Systems; a GAO report on *Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls Across Federal Agencies;* and a CRS report entitled *Cyberwarfare and Cyberterrorism: In Brief.*

Section D, "The Efficacy of Sanctions in Avoiding Hybrid Warfare and Deterring Gray Zone Threats," offers two documents that address the potential use of sanctions for these purposes: a GAO report entitled *Nonproliferation: State Should Minimize Reporting Delays That May Affect Sanctions on Trade with Iran, North Korea, and Syria* and a GAO report focusing on North Korea entitled, *North Korea Sanctions: United States Has Increased Flexibility to Impose Sanctions, but United Nations Is Impeded by a Lack of Member State Reports.*

Section E, "The Military and Law Enforcement," rounds out the volume with three documents that discuss the relationship of the U.S. military to law enforcement agencies. They are a GAO report entitled *Civil Support: DOD Is Taking Action to Strengthen Support of Civil Authorities*, a CRS report on *The '1033 Program,' Department of Defense Support to Law Enforcement*, and a CRS "Insights" piece on The *"Militarization" of Law Enforcement and the Department of Defense's "1033 Program*." While the volume's documents clearly do not provide an exhaustive examination of hybrid warfare and the Gray Zone threat, they do provide very useful information not easily accessed by the public.

A. THE SHIFTING INTERNATIONAL SECURITY ENVIRONMENT

COMMENTARY

by
Douglas C. Lovelace, Jr.

We begin this volume with an overview document that describes the broad outlines of an international security environment that fosters hybrid warfare and facilitates "Gray Zone" threats. The June 14, 2015, Congressional Research Service (CRS) report, *A Shift in the International Security Environment: Potential Implications for Defense—Issues for Congress*, argues that the international security environment has begun another major shift. The author sets a somewhat arbitrary date of 2013 as the beginning point of the shift and names the assertiveness of the People's Republic of China (PRC) in the East China Sea and the South China Sea and the illegal seizure of Crimea by the Russian Federation as the unambiguous indicators of the shift. While those two state-centric phenomena certainly shape part of the emerging international security environment, they do not define it sufficiently.

The shift in the international security environment also results from better understanding of the strengths and weaknesses of the U.S.-led global security order and the ways in which strengths can be negated or avoided and weaknesses can be exploited by a wide array of state and non-state actors. Vladimir Putin rides a wave of popular support in Russia by stoking neonationalism and many PRC national security specialists plan for China to replace the United States as the leader of the global order. But those are not the only or even the principal reasons why the environment has entered a period of hybrid warfare and Gray Zone threat. They are easily anticipated manifestations of the antibodies that were sure to result from decades-long U.S. dominance of the international security order, but there are others.

In considering the shift in the international security environment, one must also take into account North Korea's increased obstreperousness, Iran's mostly successful deceit as to its nuclear weapons and missile delivery programs, Iran's significantly increased influence in Iraq following the withdrawal of U.S. forces, the threat Hezbollah poses to Israel, the inability of the United States to prevent the ongoing catastrophe in Syria, the emergence of a seemingly unstoppable Islamic State, the relatively unfettered operation of illegal drug and human trafficking cartels on both sides of the U.S. southwestern border, the return of autocratic populist governments in Latin America, and the rise of lone-wolf terrorism within the United States, to name a few of the other emerging threats. None of these threats lend themselves to resolution through conventional warfare. In fact all are designed to avoid it. The most fundamental question is whether the

United States has the type of tools it needs to pursue its interests in this new security environment.

The author of the CRS report correctly states that from World War II emerged a clearly discernible international security environment that became known as the "Cold War." As we know, it featured two major antagonists: the U.S.-led North Atlantic Treaty Organization (NATO) and the Russia-led Warsaw Pact. While general war between the two superpowers was not as feared as it was unthinkable, the potential belligerents challenged each other through proxies and sometimes within the Gray Zone, a point the author of the CRS report seems to overlook.

At the time the Soviet Union disintegrated and the Cold War appeared to end, it became fashionable to say the world had entered the Post–Cold War Era. Of course, that label was nothing more than an acknowledgment that the Cold War had ended. It did not describe the era that followed it. A more appropriate name for the period that began when the Cold war ended would have been the Era of American Exceptionalism. While the author of the CRS report hews to the accepted lexicon of the time, he does describe the Era of American Exceptionalism fairly well. Furthermore, the features of the evolving international security environment he lists, although not exhaustive, are sufficient to give the reader an idea of what differentiates it from the eras that preceded it.

The CRS report's author's invocation of the recently released U.S. National Military Strategy to help describe the evolving security environment in more detail is appropriate, notwithstanding the deficiencies in that strategic document. We defer a discussion of its shortcomings to the next volume in this series. *A Shift in the International Security Environment: Potential Implications for Defense—Issues for Congress* serves our need in this volume to set the strategic context for the documents that follow.

DOCUMENT NO. 1

A SHIFT IN THE INTERNATIONAL SECURITY ENVIRONMENT: POTENTIAL IMPLICATIONS FOR DEFENSE—ISSUES FOR CONGRESS

CRS Report R43838

Ronald O'Rourke
Specialist in Naval Affairs

July 14, 2015

Summary

World events since late 2013 have led some observers to conclude that the international security environment has undergone a shift from the familiar post-Cold War era of the last 20–25 years, also sometimes known as the unipolar moment (with the United States as the unipolar power), to a new and different strategic situation that features, among other things, renewed great power competition and challenges to elements of the U.S.-led international order that has operated since World War II.

A previous shift in the international security environment—from the Cold War to the post-Cold War era—prompted a broad reassessment by the Department of Defense (DOD) and Congress of defense funding levels, strategy, and missions that led to numerous changes in DOD plans and programs. A new shift in the international security environment could similarly have a number of implications for U.S. defense plans and programs. Of perhaps the greatest potential significance, such a shift could lead to a change in the current overall terms of debate over U.S. defense plans and programs. Russia's seizure and annexation of Crimea, as well as subsequent Russian actions in eastern Ukraine and elsewhere in Eastern Europe, have already led to a renewed focus among policymakers on U.S. and NATO military capabilities in Europe, and on how to counter Russia's so-called hybrid warfare tactics. China's actions in the East and South China Seas have prompted a focus among policymakers on how to counter China's so-called salami-slicing tactics in those areas. A shift in the international security environment may also be generating implications for areas such as nuclear weapons, submarines and antisubmarine warfare, and DOD reliance on Russian-made components.

Policy and oversight issues for Congress include the following:

- **Shift in strategic situations.** Has there been a shift in the international security environment, and if so, what features characterize the new environment?

- **Reassessment of U.S. defense funding levels, strategy, and missions.** Should there be a reassessment of U.S. defense funding levels, strategy, and missions?
- **Congressional role in reassessment.** If there is to be such a reassessment, how should it be done, and what role should Congress play?
- **Potential effect on plans and programs.** How might such a reassessment affect the current terms of debate on U.S. defense? What might be the potential implications for U.S. defense plans and programs?

Introduction

World events since late 2013 have led some observers to conclude that the international security environment has undergone a shift from the familiar post-Cold War era of the last 20–25 years to a new and different strategic situation that features, among other things, renewed great power competition and challenges to elements of the U.S.-led international order that has operated since World War II.[1]

A previous shift in the international security environment—from the Cold War to the post-Cold War era—prompted a broad reassessment by the Department of Defense (DOD) and Congress of defense funding levels, strategy, and missions that led to numerous changes in DOD plans and programs. A new shift in the international security environment could similarly have a number of implications for U.S. defense plans and programs.

The issue for Congress is whether a shift in the international security environment has occurred, and if so, how to respond to that shift. This report briefly describes the shift in the international security environment that some observers believe has occurred, and identifies some defense-related issues for Congress that could arise from it. Congress's decisions on these issues could have significant implications for U.S. defense capabilities and funding requirements.

This report focuses on defense-related issues and does not discuss potential implications of a shift in the international security environment for other policy areas, such as foreign policy and diplomacy, trade and finance, energy, and foreign assistance. Future CRS reports may address the potential implications of a shift in the international security environment for these other policy areas or address the U.S. role in the international security environment from other analytical perspectives.

[1] The term international order generally means the combination of laws, rules, norms, and supporting institutions that shapes and helps govern international politics and economics. The U.S.-led international order established at the end of World War II, also known as the liberal international order, can be characterized as one that features, among other things, a reliance on international law rather than force or coercion as the preferred means of settling international disputes, an emphasis on human rights, an open international trading system that attempts to evolve in the direction of free trade, and the treatment of the world's oceans, international airspace, outer space, and cyberspace as international commons.

Background

Shift in International Security Environment

Overview

World events since late 2013—including Chinese actions in the East and South China Seas since November 2013[2] and Russia's seizure and annexation of Crimea in March 2014[3]—have led some observers to conclude that the international security environment has undergone a shift from the familiar post-Cold War era of the last 20–25 years, also known as the unipolar moment (with the United States as the unipolar power), to a new and different strategic situation that features, among other things, renewed great power competition and challenges to elements of the U.S.-led international order that has operated since World War II.[4]

In August 2014, outgoing Secretary of Defense Chuck Hagel referred to "the dangerous unpredictability of a world that is I think trying to define a new world order.... We are seeing a new world order being built in the early 21st Century."[5] In October 2014, Hagel stated: "I think we are living through one of these historic, defining times.... We are seeing a new world order—post-World War II, post-Soviet implosion—being built."[6]

---

[2] For discussions of these actions, see CRS Report R42784, *Maritime Territorial and Exclusive Economic Zone (EEZ) Disputes Involving China: Issues for Congress*, by Ronald O'Rourke, and CRS Report R42930, *Maritime Territorial Disputes in East Asia: Issues for Congress*, by Ben Dolven, Mark E. Manyin, and Shirley A. Kan.

[3] For discussion Russia's seizure and annexation of Crimea, see CRS Report RL33460, *Ukraine: Current Issues and U.S. Policy*, by Steven Woehrel.

[4] See, for example, Walter Russell Mead, "The End of History Ends," *The American Interest*, December 2, 2013; Paul David Miller, "Crimea Proves That Great Power Rivalry Never Left Us," *Foreign Policy*, March 21, 2014; Walter Russell Mead, "The Return of Geopolitics," *Foreign Affairs*, May/June 2014; Robert Kagan, "Superpowers Don't Get to Retire," *New Republic*, May 26, 2014; James Kitfield, "The New Great Power Triangle Tilt: China, Russia Vs. U.S.," *Breaking Defense*, June 19, 2014; Lilia Shevtsova, "Putin Ends the Interregnum," *The American Interest*, August 28, 2014; David E. Sanger, "Commitments on Three Fronts Test Obama's Foreign Policy," *New York Times*, September 3, 2014; Steven Erlanger, "NATO's Hopes for Russia Have Turned to Dismay," *New York Times*, September 12, 2014; Richard N. Haass, "The Era of Disorder," *Project Syndicate*, October 27, 2014; Bruce Jones, "What Stretgic Environment does the Transatlantic Community Confront?" German Marshall Fund of the United States, Policy Brief, January 15, 2015, 5 pp.; Garry Kasparov, "The Global War on Modernity," *Wall Street Journal*, January 20, 2015; Chester A Crocker, "The Strategic Dilemma of a World Adrift," *Survival*, February-March 2015: 7–30; Robert Kagan, "The United States Must Resist A Return to Spheres of Interest in in the International System," Brookings Institution, February 19, 2015; Richard Fontaine, "Salvaging Global Order," *The National Interest*, March 10, 2015; Philip Stephens, "Why the Business of Risk Is Booming," *Financial Times*, March 12, 2015; Stewart Patrick and Isabella Bennett, "Geopolitics Is Back—and Global Governance Is Out," *The National Interest*, May 12, 2015; "Rise of the Regional Hegemons," *Wall Street Journal*, May 25, 2015; David Barno and Nora Bensahel, "The New Chiefs in Town," *War on the Rocks*, June 30, 2015; James Kitfield, "Requiem For The Obama Doctrine," *Breaking Defense*, July 6, 2015; Aaron Mehta, "Mixed Reaction to US National Military Strategy," *Defense News*, July 12, 2015.

Some other observers see the emergence of a medieval-or feudal-like situation. See, for example, Brad Allenby, "The Return to Medievalism," *Slate*, March 18, 2015; Steven Metz, "Emerging Neo-Feudal World Leaving U.S., Global Security Behind," *World Politics Review*, May 29, 2015. See also Matt Thompson, "UN's Purpose Questioned in a 'Post-Nation' World," *Defense One*, July 1, 2015.

[5] As quoted in Chris Uhlmann, "US Secretary of Defense Says 'New World Order Being Built,'" *Australian Broadcasting Corporation*, August 11, 2014.

[6] As quoted in David A. Graham, "Defense Secretary Chuck Hagel: Get Used to Endless War," *The Atlantic*, October 29, 2014. In September 2014, Deputy Secretary of Defense Robert Work stated:

> I think there's two things happening, both with Russia and China. First, they clearly are staking out their position in their near abroads. And this is one of the things that we're going to have to work out over the course of the next several years on what they consider to be areas of their vital interest, and

Cold War Era

The Cold War, which is generally viewed as lasting from the late 1940s until the late 1980s/early 1990s, was generally viewed as a strongly bipolar situation featuring two superpowers—the United States and the Soviet Union—engaged in a political, ideological, and military competition for influence across multiple regions. The military component of that competition was often most acutely visible in Europe, where the U.S.-led NATO alliance and the Soviet-led Warsaw Pact alliance faced off against one another with large numbers of conventional forces and theater nuclear weapons, backed by longer-ranged strategic nuclear weapons.

Post-Cold War Era

The post-Cold War era, which is generally viewed as having begun in the early 1990s, tended toward a unipolar situation, with the United States as the world's sole superpower. The Warsaw Pact had disbanded, the Soviet Union had dissolved into Russia and the former Soviet republics, and neither Russia, China, nor any other country was viewed as posing a significant challenge to either the United States' status as the world's sole superpower or the U.S.-led international order. Compared to the Cold War, the post-Cold War era generally featured reduced levels of overt political, ideological, and military competition among major states. Following 9/11, the post-Cold War era was additionally characterized by a strong focus (at least from a U.S. perspective) on countering transnational terrorist organizations that had emerged as significant non-state actors, particularly Al Qaeda.

The New Situation

Some Emerging Features

Observers who conclude that the international security environment has shifted to a new strategic situation generally view the new period not as a bipolar situation (like the Cold War) or a unipolar situation (like the post-Cold War era), but as a multipolar situation characterized by renewed competition among three major world powers—the United States, China, and Russia. Other emerging characteristics of the new international security situation as viewed by these observers include the following:

- renewed ideological competition, this time against 21st-century forms of authoritarianism in Russia, China, and other countries;[7]

---

what we have to do is find a means by which to make sure that those desires do not resort to the use of force and would require an overt response militarily from us. We have to work these out and make sure that Russia and China feel secure in their near abroads. But both of those countries definitely believe that the current world order, as established over the last 70 years, they would like to change certain aspects of it. So that's going to be a constant point of attention. So at the strategic level, it is, how are we going to work with two very strong powers, regional powers right now? And how will we be able to work out ways in which we engage with each other over time?

(Department of Defense news transcript, "Deputy Secretary of Defense Work Delivers Remarks at the Council on Foreign Relations," September 30, 2014, accessed October 31, 2014, at http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5509.)

[7] See, for example, Anne Applebaum, "Russia's Anti-Western Ideology Has Global Consequences," *Washington Post*, March 28, 2014; Paula J. Dobriansky, "U.S. Needs A Strong Moral Narrative To Combat Putin," *Washington Post*, May 23, 2014; Christopher Walker, "Authoritarian Regimes Are Changing How

- the promotion in China and Russia through their state-controlled media of nationalistic historical narratives emphasizing assertions of prior humiliation or victimization by Western powers, and the use of those narratives to support revanchist or irredentist foreign policy aims;
- the use by Russia and China of new forms of aggressive or assertive military and paramilitary operations—called hybrid warfare or ambiguous warfare, among other terms, in the case of Russia's actions, and called salami-slicing tactics or gray-zone warfare, among other terms, in the case of China's actions—to gain greater degrees of control of areas on their peripheries;
- challenges by Russia and China to key elements of the U.S.-led international order, including the principle that force or threat of force should not be used as a routine or first-resort measure for settling disputes between countries, and the principle that the world's oceans are to be treated as an international commons; and
- alongside the above features, continued regional security challenges from countries such as Iran and North Korea, and a continuation of the post-Cold War era's focus (at least from a U.S. perspective) on countering transnational terrorist organizations that have emerged as significant non-state actors (now including the Islamic State organization, among other groups).

The June 2015 National Military Strategy released by the Department of Defense (DOD) states:

> Since the last National Military Strategy was published in 2011, global disorder has significantly increased while some of our comparative military advantage has begun to erode. We now face multiple, simultaneous security challenges from traditional state actors and transregional networks of sub-state groups—all taking advantage of rapid technological change. Future conflicts will come more rapidly, last longer, and take place on a much more technically challenging battlefield. They will have increasing implications to the U.S. homeland. . . .
>
> Complexity and rapid change characterize today's strategic environment, driven by globalization, the diffusion of technology, and demographic shifts. . . .
>
> Despite these changes, states remain the international system's dominant actors. They are preeminent in their capability to harness power, focus human endeavors,

The World Defines Democracy," *Washington Post*, June 13, 2014; Lilia Shevtsova, "Crowning a Winner in the Post-Crimea World," *The American Interest*, June 16, 2014; Timothy Garton Ash, "Putin's Deadly Doctrine," *New York Times*, July 18, 2014; Fareed Zakaria, "The Rise of Putinism," *Washington Post*, July 31, 2014; David Brooks, "The Battle of the Regimes," *New York Times*, August 4, 2014; Robert Tracinski, "Putinism and the 'Battle of Regimes,'" *The Federalist*, August 14, 2014; Anders Fogh Rasmussen, "The Dual Threats to Western Values," *Wall Street Journal*, September 15, 2014; Jeremy Page, "Why Russia's President Is 'Putin the Great' in China," *New York Times*, October 1, 2014; Yigal Schleifer, "Hungary At The Turning Point," *Slate*, October 3, 2014; Margit Feher, "Prompted by U.S. Comments, Hungary Insists It respects Democracy," *Wall Street Journal*, October 3, 2014; Krizstina Than, "U.S. Diplomat Criticizes PM Orban's Russia Policies," *Reuters*, October 24, 2014; Zoran Radosavljevik and Krizstina Than, "Washington Tries To Check Hungary's Drift Into Kremlin Orbit," *Reuters*, November 1, 2014; Gideon Rachman, "The West Has Lost Intellectual Self-Confidence," *Financial Times*, January 5, 2015; Garry Kasparov, "The Global War on Modernity," *Wall Street Journal*, January 20, 2015; Anna Borshchevskaya, "Moral Clarity Is Needed In Countering Anti-Western Propaganda," *Forbes*, March 14, 2015; Ellen Bork, "Democracy in Retreat," *World Affairs Journal*, May 11, 2015; Christopher Walker, "The New Containment: Undermining Democracy," *World Affairs Journal*, May/June 2015.

and provide security. Most states today—led by the United States, its allies, and partners—support the established institutions and processes dedicated to preventing conflict, respecting sovereignty, and furthering human rights. Some states, however, are attempting to revise key aspects of the international order and are acting in a manner that threatens our national security interests.

While Russia has contributed in select security areas, such as counternarcotics and counterterrorism, it also has repeatedly demonstrated that it does not respect the sovereignty of its neighbors and it is willing to use force to achieve its goals. Russia's military actions are undermining regional security directly and through proxy forces. These actions violate numerous agreements that Russia has signed in which it committed to act in accordance with international norms, including the UN Charter, Helsinki Accords, Russia-NATO Founding Act, Budapest Memorandum, and the Intermediate-Range Nuclear Forces Treaty.

Iran also poses strategic challenges to the international community. It is pursuing nuclear and missile delivery technologies despite repeated United Nations Security Council resolutions demanding that it cease such efforts. It is a state-sponsor of terrorism that has undermined stability in many nations, including Israel, Lebanon, Iraq, Syria, and Yemen. Iran's actions have destabilized the region and brought misery to countless people while denying the Iranian people the prospect of a prosperous future.

North Korea's pursuit of nuclear weapons and ballistic missile technologies also contradicts repeated demands by the international community to cease such efforts. These capabilities directly threaten its neighbors, especially the Republic of Korea and Japan. In time, they will threaten the U.S. homeland as well. North Korea also has conducted cyber attacks, including causing major damage to a U.S. corporation.

We support China's rise and encourage it to become a partner for greater international security. However, China's actions are adding tension to the Asia-Pacific region. For example, its claims to nearly the entire South China Sea are inconsistent with international law. The international community continues to call on China to settle such issues cooperatively and without coercion. China has responded with aggressive land reclamation efforts that will allow it to position military forces astride vital international sea lanes.

None of these nations are believed to be seeking direct military conflict with the United States or our allies. Nonetheless, they each pose serious security concerns which the international community is working to collectively address by way of common policies, shared messages, and coordinated action. . . .

For the past decade, our military campaigns primarily have consisted of operations against violent extremist networks. But today, and into the foreseeable future, we must pay greater attention to challenges posed by state actors. They increasingly have the capability to contest regional freedom of movement and threaten our homeland. Of particular concern are the proliferation of ballistic missiles, precision strike technologies, unmanned systems, space and cyber capabilities, and weapons of mass destruction (WMD)—technologies designed to counter U.S. military advantages and curtail access to the global commons. . . .

> Today, the probability of U.S. involvement in interstate war with a major power is assessed to be low but growing. Should one occur, however, the consequences would be immense. VEOs [violent extremist organizations], in contrast, pose an immediate threat to transregional security by coupling readily available technologies with extremist ideologies. Overlapping state and non-state violence, there exists an area of conflict where actors blend techniques, capabilities, and resources to achieve their objectives. Such "hybrid" conflicts may consist of military forces assuming a non-state identity, as Russia did in the Crimea, or involve a VEO fielding rudimentary combined arms capabilities, as ISIL has demonstrated in Iraq and Syria. Hybrid conflicts also may be comprised of state and non-state actors working together toward shared objectives, employing a wide range of weapons such as we have witnessed in eastern Ukraine. Hybrid conflicts serve to increase ambiguity, complicate decision-making, and slow the coordination of effective responses. Due to these advantages to the aggressor, it is likely that this form of conflict will persist well into the future.[8]

Markers of the Shift to the New Situation

For observers who conclude that the international security environment has shifted to a new strategic situation, the sharpest single marker of the shift arguably was Russia's seizure and annexation of Crimea in March 2014, which represented the first forcible seizure and annexation of one country's territory by another country in Europe since World War II. Other markers of the shift, such as Russia's actions in eastern Ukraine and elsewhere in Eastern Europe since March 2014, China's economic growth and military modernization over the last several years, and China's actions in the East and South China Seas over the last several years, have been more gradual and cumulative.

Some observers trace the beginnings of the argued shift in strategic situations back to 2008. In that year, Russia invaded and occupied part of the former Soviet republic of Georgia without provoking a strong cost-imposing response from the United States and its allies. Also in that year, the financial crisis and resulting deep recessions in the United States and Europe, combined with China's ability to weather that crisis and its successful staging of the 2008 Summer Olympics, are seen by observers as having contributed to a perception in China of the United States as a declining power, and to a Chinese sense of self-confidence or triumphalism.[9] China's assertive actions in the East and South China Seas can be viewed as having begun (or accelerated) soon thereafter.[10]

Comparisons to Earlier Periods

Each strategic situation features a unique combination of major actors, dimensions of competition and cooperation among those actors, and military and other technologies available to them. A new strategic situation can have some similarities to previous ones, but it will also have differences, including, potentially, one or more features not present

[8] Department of Defense, *The National Military Strategy of the United States of America 2015, The United States Military's Contribution To National Security*, June 2015, pp. i, 1–4.

[9] See, for example, Howard W. French, "China's Dangerous Game," *The Atlantic*, October 13, 2014.

[10] Some observers trace the roots of the end of the post-Cold War era further, to years prior to 2008. See, for example, Walter Russell Mead, "Who's to Blame for a World in Flames?" *The American Interest*, October 6, 2014.

in any previous strategic situation. In the early years of a new strategic situation, some of its features may be unclear, in dispute, or not yet apparent. In attempting to understand a new strategic situation, comparisons to earlier ones are potentially helpful in identifying avenues of investigation. If applied too rigidly, however, such comparisons can act as intellectual straightjackets, making it more difficult to achieve a full understanding of a new strategic situation's characteristic features, particularly those that differentiate it from previous ones.

Some observers have stated that the world is entering a new Cold War. That term may have some utility in referring specifically to U.S.-Russian relations, because the new strategic situation that some observers have identified features competition and tension with Russia. Considered more broadly, however, the Cold War was a bipolar situation, while the new environment appears to be a multipolar situation that also includes China as a major competing power. The bipolarity of the Cold War, moreover, was reinforced by the opposing NATO and Warsaw Pact alliances, whereas in contrast, Russia today does not lead an equivalent of the Warsaw Pact. And while terrorists were a concern during the Cold War, the U.S. focus on countering transnational terrorist groups was not nearly as significant during the Cold War as it has been since 9/11.

Other observers, viewing the emerging multipolar situation, have drawn comparisons to the multipolar situation that existed in the 19th century and the years prior to World War I. Still others, observing both multipolarity and the promotion in China and Russia of nationalistic historical narratives supporting revanchist or irredentist foreign policy aims, have drawn comparisons to the 1930s. Those two earlier situations, however, did not feature a strong focus on countering globally significant transnational terrorist groups, and the military and other technologies available then differ vastly from those available today. The new strategic situation that some observers have identified may be similar in some respects to previous strategic situations, but it also differs from previous situations in certain respects, and might be best understood by direct observation and identification of its key features.

Renewed Emphasis on Grand Strategy and Geopolitics

The discussion of the shift in the international security environment that some observers have identified has led to a renewed emphasis in discussions of U.S. security and foreign policy on grand strategy and geopolitics.[11] From a U.S. perspective, grand strategy

[11] See, for example, William C. Martel, "Why America Needs a Grand Strategy," *The Diplomat*, June 18, 2012; Aaron David Miller, "The Naiveté of Distance," *Foreign Policy*, March 31, 2014; Robert Kaplan, "The Gift of American Power," *Real Clear World*, May 15, 2014; William C. Martel, "America's Grand Strategy Disaster," *The National Interest*, June 9, 2014; Adam Garfinkle, "The Silent Death of American Grand Strategy," *American Review*, 2014; Christopher A. Ford, "Ending the Strategic Holiday: U.S. Grand Strategy and a 'Rising' China," *Asia Policy*, Number 18 (July 2014): 181–189; William Ruger, "A Realist's Guide to Grand Strategy," *The American Conservative*, August 26, 2014; Barry R. Posen, *Restraint: A New Foundation for U.S. Grand Strategy*, Cornell University Press, 2014, 256 pp. (Cornell Studies in Security Affairs); R. D. Hooker, *The Grand Strategy of the United States*, Washington, National Defense University Press, October 2014, 35 pp. (INSS Strategic Monograph, Institute for National Strategic Studies); F.G. Hoffman, "Grand Strategy: The Fundamental Considerations," *Orbis*, Volume 58, Issue 4 (Fall 2014), 2014: 472–485; Michael Page, "Is 'Restraint' a Realistic Grand Strategy?" *Cicero Magazine*, October 21, 2014; Bryan McGrath, "Unconstrained Grand Strategy," *War on the Rocks* October 28, 2014; Joseph Sarkisian, "American Grand Strategy or Grand Illusion?" *Cicero*, December 1, 2014; Chris Miller, "State of Disunion: America's Lack of Strategy is its Own Greatest Threat, *Cicero*, January 27, 2015; Jerry Hendrix, *Avoiding Trivia: A Strategy for Sustainment and Fiscal Responsibility*, Center for a New American Security, February 2015, 36 pp.; Jim Mattis, "A New

can be understood as strategy considered at a global or interregional level, as opposed to strategies for specific countries, regions, or issues. Geopolitics refers to the influence on international relations and strategy of basic world geographic features such as the size and location of continents, oceans, and individual countries.

From a U.S. perspective on grand strategy and geopolitics, it can be noted that most of the world's people, resources, and economic activity are located not in the Western Hemisphere, but in the other hemisphere, particularly Eurasia. In response to this basic feature of world geography, U.S. policymakers for the last several decades have chosen to pursue, as a key element of U.S. national strategy, a goal of preventing the emergence of a regional hegemon in one part of Eurasia or another, on the grounds that such a hegemon could represent a concentration of power strong enough to threaten core U.S. interests by, for example, denying the United States access to some of the other hemisphere's resources and economic activity. Although U.S. policymakers have not often stated this key national strategic goal explicitly in public, U.S. military (and diplomatic) operations in recent decades—both wartime operations and day-to-day operations—can be viewed as having been carried out in no small part in support of this key goal.

The U.S. goal of preventing the emergence of a regional hegemon in one part of Eurasia or another is a major reason why the U.S. military is structured with force elements that enable it to cross broad expanses of ocean and air space and then conduct sustained, large-scale military operations upon arrival. Force elements associated with this goal include, among other things, an Air Force with significant numbers of long-range bombers, long-range surveillance aircraft, long-range airlift aircraft, and aerial refueling tankers, and a Navy with significant numbers of aircraft carriers, nuclear-powered attack submarines, large surface combatants, large amphibious ships, and underway replenishment ships.

Congressional Participation in Reassessment of U.S. Defense During Previous Shift

A previous shift in the international security environment—from the Cold War to the post-Cold War era—prompted a broad reassessment of defense funding levels, strategy, and missions that led to numerous changes in DOD plans and programs. Many of these changes were articulated in the 1993 Bottom-Up Review (BUR),[12] a reassessment of U.S. defense plans and programs whose very name conveyed the fundamental nature of the reassessment that had occurred.[13] In general, the BUR reshaped the U.S. military into a

American Grand Strategy," Hoover Institution, February 26, 2015; Stewart Patrick and Isabella Bennett, "Geopolitics Is Back—and Global Governance Is Out," *The National Interest*, May 12, 2015; Alfred McCoy, "The Geopolitics of American Global Decline," *Real Clear World*, June 8, 2015; Steve LeVine, "How China Is Building the Biggest Commercial-Military Empire in History," *Defense One*, June 9, 2015; Thomas Vien, "The Grand Design of China's New Trade Routes," *Stratfor*, June 24, 2015; John R. Deni, "General Dunford Is Right About Russia, But Not Because of Their Nukes," *War on the Rocks*, July 13, 2015.

[12] See Department of Defense, *Report on the Bottom-Up Review*, Les Aspin, Secretary of Defense, October 1993, 109 pp.

[13] Secretary of Defense Les Aspin's introduction to DOD's report on the 1993 BUR states:

> In March 1993, I initiated a comprehensive review of the nation's defense strategy, force structure, modernization, infrastructure, and foundations. I felt that a department-wide review needed to be conducted "from the bottom up" because of the dramatic changes that have occurred in the world as a result of the end of the Cold War and the dissolution of the Soviet Union. These changes in the

force that was smaller than the Cold War U.S. military, and oriented toward a planning scenario being able to conduct two major regional contingencies (MRCs) rather than the Cold War planning scenario of a NATO-Warsaw Pact conflict.[14]

Through both committee activities and the efforts of individual Members, Congress played a significant role in the reassessment of defense funding levels, strategy, and missions that was prompted by the end of the Cold War. In terms of committee activities, the question of how to change U.S. defense plans and programs in response to the end of the Cold War was, for example, a major focus for the House and Senate Armed Services Committees in holding hearings and marking up annual national defense authorization acts in the early 1990s.[15]

In terms of efforts by individual Members, some Members put forth their own proposals for how much to reduce defense spending from the levels of the final years of the Cold War,[16] while others put forth detailed proposals for future U.S. defense strategy, plans, programs, and spending. Senator John McCain, for example, issued a detailed,

---

international security environment have fundamentally altered America's security needs. Thus, the underlying premise of the Bottom-Up Review was that we needed to reassess all of our defense concepts, plans, and programs from the ground up.

(Department of Defense, *Report on the Bottom-Up Review*, Les Aspin, Secretary of Defense, October 1993, p. iii.)

[14] For additional discussion of the results of the BUR, see CRS Report 93-839 F, *Defense Department Bottom-Up Review: Results and Issues*, October 6, 1993, 6 pp., by Edward F. Bruner, and CRS Report 93-627 F, *Defense Department Bottom-Up Review: The Process*, July 2, 1993, 9 pp., by Cedric W. Tarr, Jr. [both nondistributable and available from the author of this report].

[15] See, for example:

- the House Armed Services Committee's report on the FY1991 National Defense Authorization Act (H.Rept. 101-665 of August 3, 1990, on H.R. 4739), pp. 7–14;
- the Senate Armed Services Committee's report on the FY1991 National Defense Authorization Act (S.Rept. 101-384 of July 20 (legislative day, July 10), 1990, on S. 2884), pp. 8–36;
- the House Armed Services Committee's report on the FY1992 and FY1993 National Defense Authorization Act (H.Rept. 102-60 of May 13, 1991, on H.R. 2100), pp. 8 and 13;
- the Senate Armed Services Committee's report on the FY1992 and FY1993 National Defense Authorization Act (S.Rept. 102-113 of July 19 (legislative day, July 8), 1991, on S. 1507), pp. 8–9;
- the House Armed Services Committee's report on the FY1993 National Defense Authorization Act (H.Rept. 102-527 of May 19, 1992, on H.R. 5006), pp. 8–10, 14–15, and 22;
- the Senate Armed Services Committee's report on the FY1993 National Defense Authorization Act (S.Rept. 102-352 of July 31 (legislative day, July 23), 1992, on S. 3114), pp. 7–12;
- the House Armed Services Committee's report on the FY1994 National Defense Authorization Act (H.Rept. 103-200 of July 30, 1993, on H.R. 2401), pp. 8–9 and 18–19;
- the House Armed Services Committee's report on the FY1995 National Defense Authorization Act (H.Rept. 103-499 of May 10, 1994, on H.R. 4301), pp. 7 and 9;
- the Senate Armed Services Committee's report on the FY1995 National Defense Authorization Act (S.Rept. 103-282 of June 14 (legislative day, June 7), 1994, on S. 2182), pp. 8–9; and
- the House Armed Services Committee's report on the FY1996 National Defense Authorization Act (H.Rept. 104-131 of June 1, 1995, on H.R. 1530), pp. 6–7 and 11–12.

[16] See, for example, Clifford Krauss, "New Proposal for Military Cut," *New York Times*, January 7, 1992: A11 [discussing a proposal by Senator Phil Gramm for reducing defense spending by a certain amount]; "Sen. Mitchell Proposes $100 Billion Cut in Defense," *Aerospace Daily*, January 17, 1992: 87; John Lancaster, "Nunn Proposes 5–Year Defense Cut of $85 Billion," *Washington Post*, March 25, 1992: A4.

32-page policy paper in November 1991 presenting his proposals for defense spending, missions, force structure, and weapon acquisition programs.[17]

Perhaps the most extensive individual effort by a Member to participate in the reassessment of U.S. defense following the end of the Cold War was the one carried out by Representative Les Aspin, the chairman of the House Armed Services Committee. In early 1992, Aspin, supported by members of the committee's staff, devised a force-sizing construct and potential force levels and associated defense spending levels U.S. defense for the new post-Cold War era. A principal aim of Aspin's effort was to create an alternative to the "Base Force" plan for U.S. defense in the post-Cold War era that had been developed by the George H. W. Bush Administration.[18] Aspin's effort included a series of policy papers in January and February 1992[19] that were augmented by press releases and speeches. Aspin's policy paper of February 25, 1992, served as the basis for his testimony that same day at a hearing on future defense spending before the House Budget Committee. Although DOD and some other observers (including some Members of Congress) criticized Aspin's analysis and proposals on various grounds,[20] the effort arguably proved consequential the following year, when Aspin became Secretary of Defense in the new Clinton Administration. Aspin's 1992 effort helped inform his participation in DOD's 1993 BUR. The 1993 BUR in turn created a precedent for the Quadrennial Defense Review (QDR) process that remains in place today.

Potential or Emerging Implications for Defense

The shift in strategic situations that some observers have identified could have a number of implications for U.S. defense plans and programs, including those discussed briefly below.

[17] Senator John McCain, Matching A Peace Dividend With National Security, A New Strategy For The 1990s, November 1991, 32 pp.

[18] See, for example, "Arms Panel Chief Challenges Ending Use of Threat Analysis," *Aviation Week & Space Technology*, January 13, 1992: 28; Patrick E. Tyler, "Top Congressman Seeks Deeper Cuts in Military Budget," *New York Times*, February 23, 1991: 1; Barton Gellman, "Debate on Military's Future Crystallizes Around 'Enemies List,'" *Washington Post*, February 26, 1992: A20; Pat Towell, "Planning the Nation's Defense," *CQ*, February 29, 1992: 479. For more on the Base Force, see CRS Report 92-493 S, *National Military Strategy, The DoD Base Force, and U.S. Unified Command Plan*, June 11, 1992, 68 pp., by John M. Collins [nondistributable and available from the authors of this report].

[19] These policy papers included the following:

- National Security in the 1990s: Defining a New Basis for U.S. Military Forces, Rep. Les Aspin, Chairman, House Armed Services Committee, Before the Atlantic Council of the United States, January 6, 1992, 23 pp.;
- An Approach to Sizing American Conventional Forces For the Post-Soviet Era, Rep. Les Aspin, Chairman, House Armed Services Committee, January 24, 2991, 20 pp.;
- Tomorrow's Defense From Today's Industrial Base: Finding the Right Resource Strategy For A New Era, by Rep. Les Aspin, Chairman, House Armed Services Committee, Before the American Defense Preparedness Association, February 12, 1992, 20 pp.; and
- An Approach to Sizing American Conventional Forces For the Post-Soviet Era, Four Illustrative Options, Rep. Les Aspin, Chairman, House Armed Services Committee, February 25, 1992, 27 pp.

[20] See, for example, "Aspin Defense Budget Plans Rebuffed By Committee," *Defense Daily*, February 24, 1992: 289; "Pentagon Spurns Aspin's Budget Cuts as 'Political,'" *Washington Post*, February 28, 1992: A14.

Terms of Debate over U.S. Defense

Of perhaps the greatest potential significance, a shift from the post-Cold War era to a new strategic situation could lead to a change in the current overall terms of debate over U.S. defense plans and programs. The current terms of debate are shaped by things such as the limits on defense spending established under the Budget Control Act (BCA) of 2011 (S. 365/P.L. 112-25 of August 2, 2011) as amended, the defense strategic guidance document of January 2012,[21] and the 2014 Quadrennial Defense Review.[22] If the current terms of debate largely reflect the features of the post-Cold War era, they may not be responsive to features of the new strategic situation that some observers have identified.[23]

Some observers, citing recent world events, have raised the question of whether defense spending should be increased above levels set forth in the BCA, and consequently whether the BCA should be amended or repealed.[24] If policymakers judge that a shift in strategic situations of the kind discussed here is occurring, the nature of the U.S. response to that shift could lead to defense spending levels that are higher than, lower than, or about the same as those in the BCA.

U.S. and NATO Military Capabilities in Europe

Russia's seizure and annexation of Ukraine and Russia's subsequent actions in eastern Ukraine and elsewhere in Eastern Europe have led to a renewed focus among policymakers on U.S. and NATO military capabilities in Europe.[25] In July 2014, the Administration,

[21] Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, 8 pp. For additional discussion, see CRS Report R42146, *Assessing the January 2012 Defense Strategic Guidance (DSG): In Brief*, by Catherine Dale and Pat Towell.

[22] Department of Defense, *Quadrennial Defense Review 2014*, 64 pp. For additional discussion, see CRS Report R43403, *The 2014 Quadrennial Defense Review (QDR) and Defense Strategy: Issues for Congress*, by Catherine Dale.

[23] See, for example, David Barno and Nora Bensahel, "Addressing Tomorrow's Challenges With Yesterday's Budget," *War on the Rocks*, February 10, 2015; John Grady, "Think Tank Panel Tells House U,.S. Military Faces More Challenges, Suggests Pentagon Spending Reforms," *USNI News*, February 11, 2015.

[24] See, for example, John T. Bennett, "Could Global Threat Picture Restore US Defense Increases?" *Defense News*, August 31, 2014; Charles Lane, "The U.S. Needs To Get Serious About Defense Spending," *Washington Post*, September 3, 2014; Robert J. Samuelson, "America's Neglected Defense," *Washington Post*, September 7, 2014; Michele Flournoy and Eric Edelman, "Cuts To Defense Spending Are Hurting Our National Security," *Washington Post*, September 19, 2014; Mackenzie Eaglen, "GOP, Dems Must Rebuild Military Readiness," *Breaking Defense*, September 26, 2014; Ron Haskins and Michael O'Hanlon, "Commentary: Stop Sequestering Defense," *Defense News*, October 13, 2014; Merrill D'Arezzo, "Experts Call For National Debate On U.S. Military Priorities," *Military Times*, October 23, 2104; Martin Matishak and Rebecca Shabad, "Defense Hopes For Sequester Relief," *The Hill*, October 26, 2014; James Jay Carafano, "Is America's Defense Budget Too Small?" *The National Interest*, October 31, 2014; Thomas Donnelly and Gary Schmitt, "AWOL on the Defense Budget," *The Weekly Standard*, March 30, 2015; Dakota L. Wood, "An Epic Congressional Failure of Defense," *War on the Rocks*, May 13, 2015; Fred Hiatt, "Real World military Funding," *Washington Post*, May 17, 2015.

[25] See, for example, Wiktor Szary, "NATO Looking at Beefing Up Baltic Exercises: Top General," *Reuters*, January 13, 2015; John Vandiver and Michael Darnell, "Army Looking to Store Tanks, Equipment in Eastern Europe," Joe Gould, "US Army Talks Tanks as Russia's Hit Ukraine," *Defense News*, February 19, 2015; Agence France-Presse, "US Sends Heavy Armor to Baltic States To 'Deter' Russia," *Defense News*, March 9, 2015; Joe Gould, "US Plans Show-of-Force Exercise in E. Europe," *Defense News*, March 19, 2015; Monika Scislowska, "US Troops Drive in Eastern Europe to Show Defense Readiness," *Military.com*, March 23, 2015; Rick Lyman, "An American Military Convoy in Europe Aims to Reassure Allies," *New York Times*, March 29, 2015; Brendan McGarry, "3rd ID Soldiers to Deploy to Europe This Year in Response

as part of its FY2015 funding request for the Overseas Contingency Operations (OCO) part of DOD's budget, requested $1 billion for a European Reassurance Initiative, of which $925 million would be for DOD to carry out several force deployments and operations in Europe.[26] At the September 4–5, 2014, NATO summit in Wales, NATO leaders announced a series of initiatives for refocusing NATO away from "out of area" (i.e., beyond-Europe) operations, and back toward a focus on territorial defense and deterrence in Europe itself.[27] In December 2014, Russia issued a new military doctrine that, among other things, calls for a more assertive approach toward NATO.[28] In June 2015, Russia stated that it would respond to the placement of additional U.S. military equipment in Eastern Europe by deploying additional forces along its own western border.[29]

The increased attention that U.S. policymakers are paying to the security situation in Europe, combined with U.S. military operations in the Middle East against the Islamic State organization and similar groups, has intensified preexisting questions among some observers about whether the United States will be able to fully implement the military component of the U.S. strategic rebalancing to the Asia-Pacific region that was formally announced in the January 2012 defense strategic guidance document.

New Forms of Aggression and Assertiveness

Russia's seizure and annexation of Crimea, as well as subsequent Russian actions in eastern Ukraine and elsewhere in Eastern Europe, have already led to a renewed focus among policymakers on how to counter Russia's hybrid warfare or ambiguous warfare tactics.[30]

---

to Russia," Military.com, April 1, 2015; Aaron Mehta, "EUCOM Head: Consider Force Structure Increase," *Defense News*, April 30, 2015; Ashish Kumar Sen, "Standing Up to a 'Revanchist Russia,'" Atlantic Council, May 5, 2015; Carol J. Williams, "NATO Military Exercises Aim To Send Message of Resolve To Russia," *Los Angeles Times*, May 8, 2015; Kristina Wong, "US, Allies Flex Military Muscle in Baltic Region," *The Hill*, June 8, 2015; Michael Hoffman, "Secretary Says Air Force Could Send F-22s to Europe to Counter Russia," *Military.com*, June 15, 2015; Thomas Gibbons-Neff, "U.S. Pledges Troops and Equipment to New NATO Task Force," *Washington Post*, June 22, 105; Eric Schmitt and Steven Lee Myers, "NATO Returns Its Attention to an Old Foe, Russia," *New York Times*, June 23, 2015; Thomas Gibbons-Neff, "Pentagon to Boost Military Equipment in Europe Amid Moscow Anger," *Washington Post*, June 23, 2015; Aaron Mehta, "Pentagon Placing Gear in Eastern Europe," *Defense News*, June 23, 2015; Naftali Bendavid, "NATO Ramps Up Response to Russia," *Wall Street Journal*, June 24, 2015; John-Thor Dahlburg, "NATO Retools for Long-Haul Standoff With Russia," *Military Times*, June 24, 2015; Marcus Weisgerber, "Pentagon Moved Money to Counter Russia," *Defense One*, July 8, 2015.

[26] Prepared Statement of the Honorable Robert O. Work, Deputy Secretary of Defense, and Admiral James A. Winnefeld, Jr, USN, Vice Chairman of the Joint Chiefs of Staff, Before the House Armed Services Committee on the FY2015 Overseas Contingency Operations Budget Request for the Department of Defense, Wednesday, July 16, 2014, pp. 2, 4–5.

[27] For additional discussion, see CRS Report R43698, *NATO's Wales Summit: Outcomes and Key Challenges*, by Paul Belkin.

[28] See, for example, Jaroslaw Adamowski, "Russia Overhauls Military Doctrine," *Defense News*, January 10, 2015.

[29] Karoun Demirjian, "Russia Says It Would Match Any U.S. Military Buildup in Eastern Europe," *Washington Post*, June 15, 2015.

[30] See, for example, Jackson Diehl, "Ukraine's Wake-Up Call for NATO," *Washington Post*, April 27, 2014; Peter Pomerantsev, "How Putin Is Reinventing Warfare," *Foreign Policy*, May 5, 2014; Frank Hoffman, "On Not-So-New Warfare: Political Warfare Vs. Hybrid Threats," *War on the Rocks*, July 28, 2014; Masha Gessen, "The Putin Military Doctrine," *Slate*, August 15, 2014; Peter Apps, "'Ambiguous Warfare' Providing NATO With New Challenge," *Reuters*, August 21, 2014; Paul Huard, "'Maskirovka' Is Russian Secret War," *War Is Boring*, August 25, 2014; Sam Jones, "Ukraine: Russia's New Art of War," *Financial Times*, August 28, 2014; Uri Friedman, "Russia's Slow-Motion Invasion of Ukraine, Is Russia Waging A New Form of Warfare, Or A Very Old One?" *The Atlantic*, August 29, 2014; Matthew Gault, "NATO Is Acting Like It's 1985; Old Alliance Needs New Ideas To Combat Russian Secret War," *War Is Boring*, August 30, 2014; Jakub Grygiel

China's actions in the East and South China Seas have prompted a focus among policymakers on how to counter China's so-called salami-slicing tactics in those areas.[31]

Nuclear Weapons and Nuclear Deterrence

Russia's reassertion of its status as a major world power has included, among other things, references by Russian officials to nuclear weapons and Russia's status as a major nuclear weapon power.[32] This has led to an increased emphasis in discussions of U.S. defense and security on nuclear weapons and nuclear deterrence[33]—a development that

and A. Weiss Mitchell, "Limited War Is Back," *The National Interest*, September 1, 2014; Cathy Young, "Derangement in Moscow," *The Weekly Standard*, September 8, 2014; Peter Pomerantsev, "Russia and the Menace of Unreality," *The Atlantic*, September 9, 2015; Andrew Higgins, "Tensions Surge in Estonia Amid a Russian Replay of Cold War Tactics," *New York Times*, October 5, 2014; Joe Gould, "US Military Girds for More 'Unconventional Warfare,'" *Defense News*, October 24, 2014; Douglas Mastriano, "Defeating Putin's Strategy of Ambiguity," *War on the Rocks*, November 6, 2014; Peter Apps, "West Struggles With Russia's 'Ambiguous Warfare' Tactics," *Reuters*, November 27, 2014; Matthew Armstrong, "Russia's War in Information," *War on the Rocks*, December 15, 2014; Bill Sweetman, "Denial And Disinformation Will Shape Future Warfare," *Aviation Week & Space Technology*, December 30, 2014; Peter Pomerantsev, "The Putin Show," *Commentary*, January 1, 2015; Peter Pomerantsev, "Inside Putin's Information War," *Politico*, January 4, 2015; Tim Starks, "New House Armed Services Chairman Plans Focus on Unconventional Warfare," *Roll Call*, January 14, 2015; Edgar Buckley and Ioan Pascu, "Report Warms Russia's 'Hybrid Warfare' In Ukraine Could Inspire Others," Radio Free Europe/Radio Liberty, February 18, 2015; "NATO's Article 5 and Russian Hybrid Warfare," Atlantic Council, March 17, 2015; Agence France-Presse, "NATO Allies Brace for Russia's 'Hybrid Warfare,'" *Defense News*, March 18, 2015; Agence France-Presse, "NATO Allies Brace for Russia's 'Hybrid Warfare,'" *Defense News*, March 18, 2015; Andreas Jacobs and Guillaume Lasconjarias, "NATO's Hybrid Flanks, Handling Unconventional Warfare in the South and East," NATO Defense College, April 2015, 12 pp.; Nadia Schadlow, "The Problem With Hybrid Warfare," *War on the Rocks*, April 2, 2015; Phillip Lohaus, "Short of War: How America's Competitors Chip Away at Its Traditional military Might," *The National Interest*, May 11, 2015; Agence France-Presse, "NATO, EU To Work Against 'Hybrid Warfare,'" *Defense News*, May 14, 2015; Tod Lindberg, "The Answer to 'Hybrid Warfare,'" *The Weekly Standard*, May 18, 2015; Octavian Manea, "Post Crimea Europe: NATO In the Age of Limited Wars," *Small Wars Journal*, June 2, 2015; Thomas Gibbons-Neff, "United States to NATO: Ditch the 'Cold War Playbook,'" Washington Post, June 21, 2015.

[31] Adam Entous and Julian E. Barnes, "U.S. Beefs Up Military Options for china as Obama Reassures Allies in Asia," *Wall Street Journal*, April 27, 2014; Jackson Diehl, "China's 'Creeping Invasion,'" *Washington Post*, September 14, 2014; Joe Gould, "US Military Girds for More 'Unconventional Warfare," *Defense News*, October 24, 2014; Robert Haddick, "The Struggle for a Strategy," *U.S. Naval Institute Proceedings*, January 2015: 52–57; Tim Starks, "New House Armed Services Chairman Plans Focus on Unconventional Warfare," *Roll Call*, January 14, 2015; Michael Mazza, "US in the Asia-Pacific: Toward A More Effective Asia Strategy," *American Enterprise Institute*, January 30, 2015; Andrew Erickson, et al., "China's Menacing Sandcastles in the South China Sea," *War on the Rocks*, March 2, 2015 (a collection of short writings by several authors); Richard Fontaine, "Chinese Land Reclamation Pushes Boundaries," *Wall Street Journal*, March 3, 2015; Harry J. Kazianis, "Superpower Showdown: America Can Stop Chinese Aggression in Asia," *The National Interest*, March 6, 2015; John Schaus, "Concrete Steps for the U.S. in the South China Sea," *War on the Rocks*, March 16, 2015; David Brunnstrom, "Senators Seek U.S. Strategy to Stop China's South China Sea Reclamation," *Reuters*, March 19, 2015; Colin Clark, "US Should 'Slow' Or 'Stop' China's Island Building: SASC, Foreign Relations Leaders, *Breaking Defense*, March 19, 2015.

See also CRS Report R42784, *Maritime Territorial and Exclusive Economic Zone (EEZ) Disputes Involving China: Issues for Congress*, by Ronald O'Rourke.

[32] See, for example, Jeffrey Tayler, "Putin's Nuclear Option," *Foreign Policy*, September 4, 2014; Alexei Anishchuk, "Putin Warns U.S. Spay Over Ukraine Threatens Global Stability," Reuters, October 15, 2014; Adrian Croft, "UK Concerned Over 'Threatening' Russian Nuclear Strategy," *Reuters*, February 6, 2015; Paul Sonne, "As Tensions With West Rise, Russia Increasingly Rattles Nuclear Saber," *Wall Street Journal*, April 5, 2015; Zachary Keck, "Russia Threatens to Deploy Nuclear Weapons in Crimea," *The National Interest*, June 1, 2015.

[33] See, for example, Ralph Vartabedian and W.J. Hennigan, "NATO Nuclear Drawdown Now Seems Unlikely," *Los Angeles Times*, September 19, 2014; William J. Broad and David E. Sanger, "U.S. Ramping Up Major Renewal in Nuclear Arms," *New York Times*, September 21, 2014; Bill Sweetman,

comes at a time when DOD is in the early stages of a multi-year plan to spend scores of billions of dollars to modernize U.S. strategic nuclear deterrent forces.[34] DOD, for example, currently has plans to acquire a new class of ballistic missile submarines[35] and a new long-range bomber.[36]

Submarines and Antisubmarine Warfare

The growing capabilities and operations of China's submarine fleet,[37] combined with a stated intention by Russia to rebuild its navy (including its submarine force) and renewed Russian submarine operations (including suspected Russian submarine operations in Swedish and Finnish waters and near Scotland), have led to a renewed focus in discussions of U.S. defense and security on the value of the U.S. attack submarine force for preserving U.S. command of the seas on a global basis, and on U.S. and allied antisubmarine warfare (ASW) capabilities.[38] This could lead to an increased focus on the procurement of Virginia-class submarines[39] and ASW platforms and equipment,

"Opinion: Nuclear Deterrence Back On The Policy Menu," *Aviation Week & Space Technology*, September 29, 2014; Robert Spalding III and Adam Lowther, "It's Time to Talk About Nukes Again," *Real Clear Defense*, October 23, 2014; Gideon Rachman, "The Nuclear Gun Is Back On The Table," *Financial Times*, November 17, 2014; Elbridge Colby, "Welcome to China and America's Nuclear Nightmare," *The National Interest*, December 19, 2014; Julian Borger, "US and Russia in Danger of Returning to Era of Nuclear Rivalry," *The Guardian*, January 4, 2015; Jeffrey Lewis, "Led Zeppelin Comes to Washington," *Foreign Policy*, January 5, 2015; Anna Applebaum, "How to Make The World's Madmen Think Twice," *Washington Post*, April 2, 2015; Bill Sweetman, "Study To Recommend More Foward-Deployed Nuclear Weapons," *Aerospace Daily & Defense Report*, May 13, 2015: 4; Brian Bradley, "Nuclear Expert Calls for U.S. to Bolster Its 'Tactical' Nuke Capabilities," *NS&D Monitor*, May 15, 2015; Josh Rogin, "U.S. Weighing Punishments for Russia's Nuclear Violations," *Bloomberg View*, May 20, 2015; Destiny Albritton, "Report: U.S. Must Modernize, Update Nuclear Strategy for New Century," Washington Free Beacon, June 23, 2015.

[34] See, for example, William J. Broad and David E. Sanger, "U.S. Ramping Up Major Renewal in Nuclear Arms," *New York Times*, September 21, 2014; CRS Report RL33640, *U.S. Strategic Nuclear Forces: Background, Developments, and Issues*, by Amy F. Woolf, and Congressional Budget Office, *Projected Costs of U.S. Nuclear Forces, 2015 to 2024* January 2015, 7 pp.

[35] CRS Report R41129, *Navy Ohio Replacement (SSBN[X]) Ballistic Missile Submarine Program: Background and Issues for Congress*, by Ronald O'Rourke.

[36] CRS Report R43049, *U.S. Air Force Bomber Sustainment and Modernization: Background and Issues for Congress*, by Jeremiah Gertler.

[37] For a discussion of China's submarine fleet, see CRS Report RL33153, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress*, by Ronald O'Rourke.

[38] See, for example, Jeff W. Benson, "Opinion: A New Era in Anti-Submarine Warfare," *USNI News*, August 27, 2014; Kris Osborn, "US Navy Issues Warnings on Russia, China's Submarine Fleets, *Military.com*, September 20, 2014; Karl Ritter and Matti Huuhtanen (Associated Press), "Submarine Hunt Sends Cold War Chill Across Baltic," *Washington Post*, October 20, 2014; Kris Osborn, "CNO Warms of Advanced Russian Submarine Development," *Military.com*, October 23, 2014; James R. Holmes, "Relearning Anti-Submarine Warfare," *The Diplomat*, October 30, 2014; Sam LaGrone, "CNO Greenert: Russian Navy 'Very Busy in the Undersea Domain,'" *USNI News*, November 4, 2014; Tony Osborne, "Canadians, French, U.S. Hunt For Submarine Off Scotland," *Aerospace Daily & Defense Report*, December 9, 2014; Kylie Maclellan, "Britain Calls on NATO Allies To Help in Submarine Hunt: Media," *Reuters*, December 10, 2014; Jeffrey Lewis, "Led Zeppelin Comes to Washington," *Foreign Policy*, January 5, 2015; Jamie Merrill, "MoD Asks for American Help in Searching For Russian Submarine Near Scotland," *The Independent*, January 8, 2015; Tony Osborne, "Sweden Acknowledges Second Submarine Hunt," *Aerospace Daily & Defense Report*, January 16, 2015: 3; Marcus Weisgerber, "Pentagon Moves Money to Counter Russia," *Defense One*, July 8, 2015.

[39] For a discussion of the Virginia-class program, see CRS Report RL32418, *Navy Virginia (SSN-774) Class Attack Submarine Procurement: Background and Issues for Congress*, by Ronald O'Rourke.

including (to cite just two examples), P-8 Poseidon multi-mission aircraft and ASW equipment for Littoral Combat Ships (LCSs).[40]

Reliance on Russian-Made Components

Increased tensions with Russia have led to an interest in eliminating instances of being dependent on Russian-made military systems and components for U.S. military systems. A current case in point concerns the Russian-made RD-180 rocket engine, which is incorporated into U.S. space launch rockets, including rockets used by DOD to put military payloads into orbit.[41]

Issues for Congress

Potential policy and oversight issues for Congress include the following:

- **Shift in strategic situation.** Has there been a shift in the international security environment, and if so, what features characterize the new environment?
- **Reassessment of U.S. defense funding levels, strategy, and missions.** Should there be a reassessment of U.S. defense funding levels, strategy, and missions?
- **Congressional role in reassessment.** If there is to be such a reassessment, how should it be done, and what role should Congress play? Should Congress conduct the reassessment itself, through committee activities? Should Congress establish the terms of reference for a reassessment to be conducted by the executive branch or by an independent, third-party entity (such as a blue ribbon panel)? Should some combination of these approaches be employed?
- **Potential effect on plans and programs.** How might such a reassessment affect the current terms of debate on U.S. defense? What might be the potential implications for U.S. defense plans and programs?
- **U.S. and NATO military capabilities in Europe.** Are the United States and its NATO allies taking appropriate steps regarding U.S. and NATO military capabilities and operations in Europe? What potential impacts would a strengthened U.S. military presence in Europe have on total U.S. military force structure requirements? What impact would it have on DOD's ability to implement the military component of the U.S. strategic rebalancing toward the Asia-Pacific region?
- **New forms of aggression and assertiveness.** Do the United States and its allies and partners have an adequate strategy for countering Russia's so-called hybrid warfare in eastern Ukraine and China's so-called salami-slicing tactics in the East and South China Seas?
- **Nuclear weapons and nuclear deterrence.** Are current DOD plans for modernizing U.S. strategic nuclear weapons, and for numbers and basing of non-strategic

[40] For a discussion of the LCS program, see CRS Report RL33741, *Navy Littoral Combat Ship (LCS)/Frigate Program: Background and Issues for Congress*, by Ronald O'Rourke.

[41] For a discussion, see CRS Report IN10069, *Russian Sanctions Reprisal Against the RD-180 Rocket Engine: Paths Ahead for U.S. National Security Space Launch*, by Steven A. Hildreth. See also Daniel Goure, "With A New Cold War Beginning, Reliance On Russia For Rocket Engines Is Madness," *Lexington Institute*, August 7, 2014; David A. Deptula, "The Russians Have Us Over a Rocket," *Wall Street Journal*, October 23, 2014.

(i.e., theater-range) nuclear weapons aligned with the needs of the new strategic situation?

- **Submarines and antisubmarine warfare.** Are current Navy plans for numbers and capabilities of attack submarines, and ASW capabilities, aligned with the needs of the new strategic situation?
- **Reliance on Russian-made components.** Aside from the Russian-made RD-180 rocket engine, what other Russian-made components, if any, are incorporated into DOD equipment? What are DOD's plans regarding reliance on Russian-made components for DOD equipment?

Legislative Activity in 2015

The Administration's proposed FY2016 defense budget was submitted to Congress on February 2, 2015.

FY2016 National Defense Authorization Act (H.R. 1735/S. 1376)

House (Committee Report)

Section 1088 of H.R. 1735 as reported by the House Armed Services Committee (H.Rept. 114-102 of May 5, 2015) states:

> SEC. 1088. Department of Defense strategy for countering unconventional warfare.
>
> (a) Strategy required.—The Secretary of Defense, in consultation with the President and the Chairman of the Joint Chiefs of Staff, shall develop a strategy for the Department of Defense to counter unconventional warfare threats posed by adversarial state and non-state actors.
>
> (b) Elements.—The strategy required under subsection (a) shall include each of the following:
>
> (1) An articulation of the activities that constitute unconventional warfare being waged upon the United States and allies.
>
> (2) A clarification of the roles and responsibilities of the Department of Defense in providing indications and warning of, and protection against, acts of unconventional warfare.
>
> (3) The current status of authorities and command structures related to countering unconventional warfare.
>
> (4) An articulation of the goals and objectives of the Department of Defense with respect to countering unconventional warfare threats.
>
> (5) An articulation of related or required interagency capabilities and whole-of-Government activities required by the Department of Defense to support a counter-unconventional warfare strategy.
>
> (6) Recommendations for improving the counter-unconventional warfare capabilities, authorities, and command structures of the Department of Defense.

(7) Recommendations for improving interagency coordination and support mechanisms with respect to countering unconventional warfare threats.

(8) Recommendations for the establishment of joint doctrine to support counter-unconventional warfare capabilities within the Department of Defense.

(9) Any other matters the Secretary of Defense and the Chairman of the Joint Chiefs of Staff determine necessary.

(c) Submittal to Congress.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees the strategy required by subsection (a). The strategy shall be submitted in unclassified form, but may include a classified annex.

(d) Definition of unconventional warfare.—In this section, the term "unconventional warfare" means activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, or guerrilla force in a denied area.

Section 1531 of H.R. 1735 as reported by the committee states:

SEC. 1531. Statement of policy regarding European Reassurance Initiative.

(a) Findings.—Congress makes the following findings:

(1) In February 2015, Lieutenant General James Clapper (retired), Director of National Intelligence, testified to the Committee on Armed Services of the Senate that "Russian dominance over the former Soviet space is Russia's highest foreign policy goal".

(2) Russia, under the direction of President Vladimir Putin, has demonstrated its intent to expand its sphere of influence beyond its borders and limit Western influence in the region.

(3) The Russian military is aggressively postured on the Ukrainian boarder and continues its buildup of military personnel and material. These aggressive and unwarranted actions serve to intimidate, with a show of force, the Ukrainian people as well as the other nations in the region including Georgia, the Baltic States, and the Balkan States.

(4) In December 2014, Congress enacted the Ukraine Freedom Support Act of 2014 (Public Law 113–272), which gives the President the authority to expand assistance to Ukraine, increase economic sanctions on Russia, and provide equipment to counter offensive weapons.

(5) In February 2015, the Atlantic Council, the Brookings Institute, and the Chicago Council on Global Affairs published a report entitled "Preserving Ukraine's Independence, Resisting Russian Aggression: What the United States and NATO Must Do" advocating for increased United States assistance to Ukraine with nonlethal and lethal defensive equipment.

(6) Despite Russia signing the February 2015 Minsk Agreement, it has continued to violate the terms of the agreement, as noted by Assistant

Secretary of State for European and Eurasian Affairs, Victoria Nuland, at the German Marshall Fund Brussels Forum in March 2015: "We've seen month on month, more lethal weaponry of a higher caliber . . . poured into Ukraine by the separatist Russian allies . . . the number one thing is for Russia to stop sending arms over the border so we can have real politics."

(7) The military of the Russian Federation continues to increase their show of force globally, including frequent international military flights, frequent snap exercises of thousands of Russian troops, increased global naval presence, and the threat of the use of nuclear weapons in defense of the annexation of Crimea in March 2014.

(8) The Government of the Russian Federation continues to exert and increase undue influence on the free will of sovereign nations and people with intimidation tactics, covert operations, cyber warfare, and other unconventional methods.

(9) In testimony to the Committee on Armed Services of the House of Representatives in February 2015, Commander of European Command, General Philip Breedlove, United States Air Force, stated that "Russia has employed 'hybrid warfare' . . . to illegally seize Crimea, foment separatist fever in several sovereign nations, and maintain frozen conflicts within its so-called 'sphere of influence' or 'near abroad'".

(10) The use of unconventional methods of warfare by Russia presents challenges to the United States and its partners and allies in addressing the threat.

(11) An enhanced United States military presence and readiness posture and the provision of security assistance in Europe are key elements to deterring further Russian aggression and reassuring United States allies and partners.

(12) In the National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291), Congress authorized and appropriated $1 billion for the European Reassurance Initiative, which supports Operation Atlantic Resolve of the United States Armed Forces.

(13) The European Reassurance Initiative expands United States military presence in Europe, through—

(A) bolstered and continual United States military presence;

(B) bilateral and multilateral exercises with partners and allies;

(C) improved infrastructure;

(D) increased prepositioning of United States equipment throughout Europe; and

(E) building partnership capacity for allies and partners.

(14) The European Reassurance Initiative has served as a valuable tool in strengthening the partnerships with the North Atlantic Treaty Organization (NATO) as well as partnerships with non-member allies in the region.

(15) As a result of the NATO 2014 Summit in Wales, NATO has initiated a Readiness Action Plan to increase partner nation funding and resourcing to combat Russian aggression. NATO's efforts with the Readiness Action Plan and United States investment in regional security through the European Reassurance Initiative will serve to continue and reinforce the strength and fortitude of the alliance against nefarious actors.

(16) The President's Budget Request for fiscal year 2016 includes $789.3 million to continue the European Reassurance Initiative focus on increased United States military troop rotations in support of Operation Atlantic Resolve, maintaining and further expanding increasing regional exercises, and building partnership capacity.

(b) Statement of policy.—It is the policy of the United States to continue and expand its efforts in Europe to reassure United States allies and partners and deter further aggression and intimidation by the Russian Government, in order to enhance security and stability in the region. This policy shall include—

(1) continued use of conventional methods, including increased United States military presence in Europe, exercises and training with allies and partners, increasing infrastructure, prepositioning of United States military equipment in Europe, and building partnership capacity;

(2) increased emphasis on countering unconventional warfare methods in areas such as cyber warfare, economic warfare, information operations, and intelligence operations, including increased efforts in the development of strategy, operational concepts, capabilities, and technologies; and

(3) increased security assistance to allies and partners in Europe, including the provision of both non-lethal equipment and lethal equipment of a defensive nature to Ukraine.

Section 1610 of H.R. 1735 as reported by the committee states:

SEC. 1610. Prohibition on reliance on China and Russia for space-based weather data.

(a) Prohibition.—The Secretary of Defense shall ensure that the Department of Defense does not rely on, or in the future plan to rely on, space-based weather data provided by the Government of China, the Government of Russia, or an entity owned or controlled by the Government of China or the Government of Russia for national security purposes.

(b) Certification.—Not later than 90 days after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees a certification that the Secretary is in compliance with the prohibition under subsection (a).

H.Rept. 114-102 states:

Russian Unconventional Warfare

Tactics employed by the Russian Federation in its aggression against Ukraine are not unique. However, Russia has combined them in new, effective, and troubling ways. It has fomented and taken advantage of ethnic disputes to

train, build, and equip a separatist army in Ukraine under Russian direction. It has combined this line of effort with propaganda, diplomatic, and economic measures to try to reduce the effectiveness of Ukraine's response, as well as the response of the United States and Europe, and to preserve and extend its perceived sphere of influence.

The North Atlantic Treaty Organization (NATO) is the most successful military alliance in history, defending the security interests of its members against external threats for over 60 years. The committee supports the NATO alliance and believes that it can successfully continue to serve as a bedrock for U.S. and European security. However, the committee notes that the methods currently being used by Russia in Ukraine pose a challenge to the NATO system.

The core of the NATO alliance is provided by Article 5 of the Washington Treaty, which enshrines the principle of collective selfdefense: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all…" In the wake of Russian actions in Ukraine, both the United States, in a series of bilateral actions referred to as the European Reassurance Initiative, and NATO collectively, in the Readiness Action Plan, have taken steps to ensure that all parties are postured to respond to any new aggression. The committee is concerned, however, that these steps may not sufficiently address the challenges posed by Russian tactics.

At its core, collective self-defense requires that the parties to the treaty agree that one of the members is under attack. This implies that such aggression can be correctly attributed to some actor outside the alliance. Russia's actions have been designed to be deniable and difficult to attribute directly to Russian government activity. Should similar tactics, or even more covert methods, be applied to NATO member states that border Russia, it may be difficult to attribute them to Russian activity and therefore difficult to trigger a collective NATO response. It is likely that some NATO members will have different views on the degree of Russian involvement. In addition, it is possible that Russia would perceive NATO may have difficulty in coming to an agreement about a collective response, which could undermine NATO's ability to deter Russia from engaging in attempts to intervene in sovereign issues of NATO members.

The committee believes that the Department of Defense, and NATO, should fully explore how the United States, NATO, and member states can, as necessary, establish deterrence mechanisms against activities such as those undertaken by the Russian government in Ukraine. The committee directs the Secretary of Defense, acting through the Office of Net Assessment or other such organization as the Secretary considers appropriate, to undertake a study exploring various strategies for deterring external efforts to interfere with the internal workings of NATO member states by Russia, or any other actor utilizing tactics such as propaganda in media, economic warfare, cyber warfare, criminal acts, and intelligence operations, similar to those being used by Russia in Ukraine. The committee expects the Secretary to deliver a report

to the congressional defense committees containing the findings of such study not later than March 31, 2016.

This study would complement a provision contained elsewhere in this Act requiring the Secretary of Defense to develop a strategy for the Department of Defense to counter unconventional warfare threats posed by adversarial state and non-state actors. (Pages 257–258)

H.Rept. 114-102 also states:

Funding and Support for the European Reassurance Initiative

The budget request included $789.3 million for the European Reassurance Initiative (ERI). The committee supports the policy and activities contained in the ERI, which was originally proposed as part of the budget request for fiscal year 2015. However, the committee observes that these initiatives are largely focused on conventional reassurance and deterrence activities. The committee also recognizes that the Russian Federation has employed unconventional warfare methods in areas such as cyber warfare, economic warfare, information operations, and intelligence operations, and believes the Department of Defense should increase its focus on countering such methods.

The committee believes that ERI funds for fiscal year 2016 should be allocated for continued conventional reassurance and deterrence activities, as outlined in section 1535 of the Carl Levin and Howard P. ''Buck'' McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291), as well as countering unconventional threats. Therefore, elsewhere in this Act, the committee includes a provision that would: (1) lay out a statement of policy regarding ERI; (2) require a Department of Defense strategy to address unconventional warfare methods; and (3) authorize increased funding for U.S. intelligence and warning capabilities related to the European theater, technologies supporting U.S. information operations and strategic communications activities, the Javelin weapon system, and Stryker combat vehicle upgrades to meet U.S. Army Europe operational needs.

The committee further believes that, as part of the U.S. effort to increase security assistance to allies and partners in Europe, ERI funds should be allocated to provide both nonlethal equipment and lethal equipment of a defensive nature to Ukraine. Therefore, elsewhere in this Act, the committee includes a provision that would authorize appropriations to provide sustainment and assistance to the military and national security forces of Ukraine.

The committee believes that all of these U.S. efforts taken in combination are vital to address regional security and to deter and counter continued Russian aggression. The committee further believes that these efforts should be enduring and must be sustained as core activities of the Department of Defense in Europe. (Pages 281–282)

House (Floor Action)

On May 15, 2015, as part of its consideration of H.R. 1735, the House agreed by voice vote to H.Amdt. 229, an en bloc amendment that included, among other things, an

amendment that was number 59 in H.Rept. 114-112 of May 13, 2015, on H.Res. 260, providing for the further consideration of H.R. 1735. Amendment number 59 in H.Rept. 115-102 states:

> Page 227, after line 19, insert the following new section:
>
> SEC. 569. REPORT ON CIVILIAN AND MILITARY EDUCATION TO RESPOND TO FUTURE THREATS.
>
> (a) IN GENERAL.—Not later than June 1, 2016, the Secretary of Defense shall submit to the congressional defense committees a report describing both civilian and military education requirements necessary to meet any threats anticipated in the future security environment as described in the quadrennial defense review. Such report shall include—
>
> (1) an assessment of the learning outcomes required of future members of the Armed Forces and senior military leaders to meet such threats;
>
> (2) an assessment of the shortfalls in current professional military education requirements in meeting such threats;
>
> (3) an assessment of successful professional military education programs that further the ability of the Department of Defense to meet such threats;
>
> (4) recommendations of subjects to be covered by civilian elementary and secondary schools in order to better prepare students for potential military service;
>
> (5) recommendations of subjects to be included in professional military education programs;
>
> (6) recommendations on whether partnerships between the Department of Defense and private institutions of higher education (as defined in section 101(a) of the Higher Education Act of 1965 (20 U.S.C. 1001(a))) would help meet such threats; and
>
> (7) an identification of opportunities for the United States to strengthen its leadership role in the future security environment and a description of how the recommendations made in this report contribute to capitalizing on such opportunities.
>
> (b) UPDATED REPORTS.—Not later than 10 months after date of the publication of each subsequent quadrennial defense review, the Secretary of Defense shall update the report described under subsection (a) and shall submit such report to the congressional defense committees.

The above section became **Section 570** of H.R. 1735 as passed by the House on May 15, 2015.

Also on May 15, 2015, as part of its consideration of H.R. 1735, the House agreed by voice vote to H.Amdt. 236, an en bloc amendment that included, among other things, an amendment that was number 115 in H.Rept. 114-112 of May 13, 2015, on H.Res. 260,

providing for the further consideration of H.R. 1735. Amendment number 115 in H.Rept. 115-102 states:

At the end of subtitle G of title XII (page 622, after line 22), add the following:

SEC. 12xx. REPORT ON IMPACT OF ANY SIGNIFICANT REDUCTION IN UNITED STATES TROOP LEVELS OR MATERIEL IN EUROPE ON NATO'S ABILITY TO CREDIBLY ADDRESS EXTERNAL THREATS TO ANY NATO MEMBER STATE.

(a) SENSE OF CONGRESS.—It is the sense of Congress that—(1) in order to demonstrate United States commitment to North Atlantic Treaty Organization (NATO) allies, especially those NATO allies under pressure on the Eastern flank of the Alliance, and to enhance the United States deterrent presence and resolve to countering threats to NATO's collective security, United States Armed Forces stationed and deployed in Europe should be increased in number and combat power; and (2) the ''current and foreseeable security environment'', as referenced in paragraph 12 of Section IV on Political-Military Matters of the Founding Act on Mutual Relations, Cooperation and Security between NATO and the Russian Federation (NATO-Russia Founding Act), has changed significantly since the signing of such Act in 1997 and thus such Act should not be read, interpreted, or implemented so as to constrain or in any way limit additional permanent stationing of substantial combat forces anywhere on the territory of any NATO member State in furtherance of NATO's core mission of collective defense and other missions.

(b) REPORT.—

(1) IN GENERAL.—In order to ensure that the United States contribution to NATO's core mission of collective defense remains robust and ready to meet any future challenges, the Secretary of Defense shall submit to the appropriate congressional committees a report on the impact of any significant reduction in United States troop levels or materiel in Europe on NATO's ability to credibly deter, resist, and, if necessary, repel external threats to any NATO member State.

(2) DEADLINE.—The report required under paragraph (1) shall be submitted not later than 30 days prior to the date on which any significant reduction described in paragraph (1) is scheduled to take place.

(3) FORM.—The report required under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex if necessary to protect the national security interests of the United States.

(4) DEFINITION.—In this subsection, the term ''appropriate congressional committees'' means—

(A) the Committee on Armed Services and the Committee on Foreign Relations of the Senate; and

(B) the Committee on Armed Services and the Committee on Foreign Affairs of the House of Representatives.

The above section became **Section 1274** of H.R. 1735 as passed by the House on May 15, 2015.

Senate

Section 212 of S. 1376 as reported by the Senate Armed Services Committee (S.Rept. 114-49 of May 19, 2015) states:

> SEC. 212. Department of Defense technology offset program to build and maintain the military technological superiority of the United States.
>
> (a) Program established.—
>
> (1) IN GENERAL.—The Secretary of Defense shall establish a technology offset program to build and maintain the military technological superiority of the United States by—
>
> (A) accelerating the fielding of offset technologies that would help counter technological advantages of potential adversaries of the United States, including directed energy, low-cost, high-speed munitions, autonomous systems, undersea warfare, cyber technology, and intelligence data analytics, developed using Department of Defense research funding and accelerating the commercialization of such technologies; and
>
> (B) developing and implementing new policies and acquisition and business practices.
>
> (2) GUIDELINES.—Not later than one year after the date of the enactment of this Act, the Secretary shall issue guidelines for the operation of the program, including—
>
> (A) criteria for an application for funding by a military department, defense agency, or a combatant command;
>
> (B) the purposes for which such a department, agency, or command may apply for funds and appropriate requirements for technology development or commercialization to be supported using program funds;
>
> (C) the priorities, if any, to be provided to field or commercialize offset technologies developed by certain types of Department research funding; and
>
> (D) criteria for evaluation of an application for funding or changes to policies or acquisition and business practices by a department, agency, or command for purposes of the program.
>
> (b) Development of directed energy strategy.—
>
> (1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Secretary, in consultation with such officials and third-party experts as the Secretary considers appropriate, shall develop a directed energy strategy to ensure that the United States directed energy technologies are being developed and deployed at an accelerated pace.

(2) COMPONENTS OF STRATEGY.—The strategy required by paragraph (1) shall include the following:

(A) A technology roadmap for directed energy that can be used to manage and assess investments and policies of the Department in this high priority technology area.

(B) Proposals for legislative and administrative action to improve the ability of the Department to develop and deploy technologies and capabilities consistent with the directed energy strategy.

(C) An approach to program management that is designed to accelerate operational prototyping of directed energy technologies and develop cost-effective, real-world military applications for such technologies.

(3) BIENNIAL REVISIONS.—Not less frequently than once every 2 years, the Secretary shall revise the strategy required by paragraph (1).

(4) SUBMITTAL TO CONGRESS.—(A) Not later than 90 days after the date on which the Secretary completes the development of the strategy required by paragraph (1) and not later than 90 days after the date on which the Secretary completes a revision to such strategy under paragraph (3), the Secretary shall submit to the Committee on Armed Services of the Senate and the Committee on Armed Services of the House of Representatives a copy of such strategy.

(B) The strategy submitted under subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(c) Applications for funding.—

(1) IN GENERAL.—Under the program, the Secretary shall, not less frequently than annually, solicit from the heads of the military departments, the defense agencies, and the combatant commands applications for funding to be used to enter into contracts, cooperative agreements, or other transaction agreements entered into pursuant to section 845 of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103–160; 10 U.S.C. 2371 note) with appropriate entities for the fielding or commercialization of technologies.

(2) TREATMENT PURSUANT TO CERTAIN CONGRESSIONAL RULES.—Nothing in this section shall be interpreted to require any official of the Department of Defense to provide funding under this section to any earmark as defined pursuant to House Rule XXI, clause 9, or any congressionally directed spending item as defined pursuant to Senate Rule XLIV, paragraph 5.

(d) Funding.—

(1) IN GENERAL.—Subject to the availability of appropriations for such purpose, of the amounts authorized to be appropriated for research, development, test, and evaluation, Defense-wide for fiscal year 2016, not more than $400,000,000 may be used for any such fiscal year for the program established under subsection (a).

(2) AMOUNT FOR DIRECTED ENERGY.—Of this amount, not more than $200,000,000 may be used for activities in the field of directed energy.

(e) Transfer authority.—

(1) IN GENERAL.—The Secretary may transfer funds available for the program to the research, development, test, and evaluation accounts of a military department, defense agency, or a combatant command pursuant to an application, or any part of an application, that the Secretary determines would support the purposes of the program.

(2) SUPPLEMENT NOT SUPPLANT.—The transfer authority provided in this subsection is in addition to any other transfer authority available to the Department of Defense.

(f) Termination.—

(1) IN GENERAL.—The authority to carry out a program under this section shall terminate on September 30, 2020.

(2) TRANSFER AFTER TERMINATION.—Any amounts made available for the program that remain available for obligation on the date the program terminates may be transferred under subsection (e) during the 180-day period beginning on the date of the termination of the program.

Regarding Section 212, S.Rept. 114-49 states:

Department of Defense technology offset program to build and maintain the military technological superiority of the United States (sec. 212)

The committee notes with concern that the United States has not faced a more diverse and complex array of crises since the end of World War II, and that taken together, they constitute the greatest challenge in a generation to the integrity of the liberal world order, which has consistently been underwritten by U.S. military technological superiority. At the same time, the committee is alarmed by the apparent erosion in recent years of this technological advantage, which is in danger of disappearing altogether. To prevent such a scenario and to maintain the country's global military technological edge, the committee recommends a provision that would establish a new $400.0 million initiative.

In doing so, the committee notes that the Defense Department is facing an emerging innovation gap. Commercial research and development in the United States now represents 80 percent of the national total, and the top four U.S. defense contractors combined spend only one-quarter of what the single biggest internet company does on research and development. Furthermore, global research and development is now more than twice that of the United States. The committee also notes that defense innovation is moving too slowly—in cycles that can last up to 18 years, whereas commercial innovation can be measured in cycles of 18 months or less.

The committee understands that accessing sources of innovation beyond the Defense Department is critical for national security, particularly in the areas of directed energy, low-cost high-speed munitions, cyber capabilities, autonomous systems, undersea warfare, and intelligence data analytics. However, there are

currently too many barriers that limit cooperation with U.S. allies and global commercial firms, posing a threat to the country's future military technological dominance.

For the past several years, U.S. adversaries have been rapidly improving their own military capabilities to counter our unique advantages. Structural trends, such as the diffusion of certain advanced military technologies, pose new operational challenges to U.S. armed forces. As a result, the dominance of the United States military can no longer be taken for granted. Consequently, the Department of Defense must remain focused on the myriad potential threats of the future and thus maintain technological superiority against potential adversaries.

The committee notes that since 1960, the department has invested more than $6.0 billion in directed energy science and technology initiatives. The committee is concerned that, despite this significant investment, the department's directed energy initiatives are not resourced at levels necessary to transition them to fullscale acquisition programs. The committee is encouraged by the Navy's demonstration a 100–150 kilowatt prototype laser and by the Air Force's demonstration of high-powered electromagnetic weapons capabilities. However, the committee is concerned about the future of directed energy technologies as a whole. The committee notes that there is no inter-service entity dedicated to advancing promising directed energy platforms beyond the development point towards acquisition.

The committee is encouraged that the department established a department-wide Defense Innovation Initiative in November 2014 to pursue innovative ways to sustain and advance our military superiority and to improve business operations throughout the department. However, the committee is concerned by the possibility that this initiative is not being implemented in an appropriate and expeditious manner.

In response to these factors, the committee recommends a provision that would establish an initiative within the Department of Defense to maintain and enhance the military technological superiority of the United States. The provision would establish a program to accelerate the fielding of offset technologies, including, but not limited to, directed energy, low-cost high-speed munitions, autonomous systems, undersea warfare, cyber technology, and intelligence data analytics, developed by the department and to accelerate the commercialization of such technologies. As part of this program, the committee expects that the Secretary of Defense would also establish updated policies and new acquisition and management practices that would speed the delivery of offset technologies into operational use.

The provision would authorize $400.0 million for fiscal year 2016 for the initiative, of which $200.0 million would be authorized specifically for directed energy technology. Accordingly, the provision would mandate the Secretary to develop a directed energy strategy to ensure that appropriate technologies are developed and deployed at an accelerated pace, and update it every 2 years. The committee expects that this strategy would include a recommendation on rationalizing the roles and authorities of the Joint Technology Office for High Energy Lasers. The provision would further direct the Secretary to submit this strategy to the Senate

Armed Services Committee and the House Armed Services Committee no later than 90 days after completing the strategy, and biennially thereafter.

To speed up the development of these vitally needed national security capabilities, the committee directs that the Secretary of Defense shall consider all appropriate flexible acquisition authorities granted in law and in this Act. These should include the management structure and streamlined procedures for rapid prototyping outlined in section 803 of this Act on the middle tier of acquisition for rapid prototyping and rapid fielding, and the procedures and authorities to be considered under section 805 of this Act on use of alternative acquisition paths to acquire critical national security capabilities to include other transactions, rapid acquisition, and commercial item authorities.

The committee expects that the Secretary of Defense would keep the Senate Committee on Armed Services and the House Committee on Armed Services regularly updated on progress of activities under this technology offsets initiative. (Pages 44–46)

Section 1253 of S. 1376 as reported by the committee states:

SEC. 1253. Increased presence of United States ground forces in Eastern Europe to deter aggression on the border of the North Atlantic Treaty Organization.

(a) Sense of Congress.—It is the sense of Congress that—

(1) the increased presence of United States and allied ground forces in Eastern Europe since April 2014 has provided a level of reassurance to North Atlantic Treaty Organization (NATO) members in the region and strengthened the capability of the Organization to respond to any potential Russian aggression against Organization members;

(2) at the North Atlantic Treaty Organization Wales summit in September 2014 member countries agreed on a Readiness Action Plan which is intended to improve the ability of the Organization to respond quickly and effectively to security threats on the borders of the Organization, including in Eastern Europe, and the challenges posed by hybrid warfare;

(3) the capability of the North Atlantic Treaty Organization to respond to threats on the eastern border of the Organization would be enhanced by a more sustained presence on the ground of Organization forces on the territories of Organization members in Eastern Europe; and

(4) an increased presence of United States ground forces in Eastern Europe should be matched by an increased force presence of European allies.

(b) Report.—

(1) IN GENERAL.—Not later than 120 days after the date of the enactment of this Act, the Secretary of Defense shall, in consultation with the Secretary of State, submit to the congressional defense committees a report setting forth an assessment of options for expanding the presence of United States ground forces of the size of a Brigade Combat Team in Eastern Europe to respond, along with European allies and partners, to the security challenges posed by Russia and increase the combat capability of forces able to

respond to unconventional or hybrid warfare tactics such as those used by the Russian Federation in Crimea and Eastern Ukraine.

(2) ELEMENTS.—The report under this subsection shall include the following:

(A) An evaluation of the optimal location or locations of the enhanced ground force presence described in paragraph (1) that considers such factors as—

(i) proximity, suitability, and availability of maneuver and gunnery training areas;

(ii) transportation capabilities;

(iii) availability of facilities, including for potential equipment storage and prepositioning;

(iv) ability to conduct multinational training and exercises;

(v) a site or sites for prepositioning of equipment, a rotational presence or permanent presence of troops, or a combination of options; and

(vi) costs.

(B) A description of any initiatives by other members of the North Atlantic Treaty Organization, or other European allies and partners, for enhancing force presence on a permanent or rotational basis in Eastern Europe to match or exceed the potential increased presence of United States ground forces in the region.

Regarding Section 1253, S.Rept. 114-49 states:

Increased presence of United States ground forces in Eastern Europe to deter aggression on the border of the North Atlantic Treaty Organization (sec. 1253)

The committee recommends a provision that would require a report to the congressional defense committees, not later than 120 days after the date of the enactment of this Act, by the Secretary of Defense, in consultation with the Secretary of State, assessing options for expanding the presence of U.S. ground forces of the size of a brigade combat team in Eastern Europe to respond, along with European allies and partners, to the security challenges posed by Russia and to increase the combat capability of allied forces to respond to unconventional or hybrid warfare tactics like those used by Russia in Crimea and eastern Ukraine. The committee believes that any increases in the presence of U.S. ground forces in Eastern Europe should be matched by similar increases in the commitment of ground forces by European allies and partners for these purposes. (Page 233)

Section 1254 of S. 1376 as reported by the committee states:

SEC. 1254. Sense of Congress on European defense and North Atlantic Treaty Organization spending.

(a) Findings.—Congress makes the following findings:

(1) North Atlantic Treaty Organization (NATO) countries, at the 2014 North Atlantic Treaty Organization Summit in Wales, pledged to "reverse the trend of declining defense budgets, to make the most effective use of our funds and to further a more balanced sharing of costs and responsibilities".

(2) Former Secretary of Defense Chuck Hagel stated on May 2, 2014, that "[t]oday, America's GDP is smaller than the combined GDPs of our 27 NATO allies. But America's defense spending is three times our Allies' combined defense spending. Over time, this lopsided burden threatens NATO's integrity, cohesion, and capability, and ultimately both European and transatlantic security".

(3) Former North Atlantic Treaty Organization Secretary General Anders Fogh Rasmussen stated on July 3, 2014, that "[d]uring the last five years, Russia has increased defense spending by 50 percent, while NATO allies on average have decrease their defense spending by 20 percent. That is not sustainable, we need more investment in defense and security".

(b) Sense of Congress.—It is the sense of Congress that—

(1) it is in the national security and fiscal interests of the United States that prompt efforts should be undertaken by North Atlantic Treaty Organization allies to meet defense budget commitments made in Declaration 14 of the Wales Summit Declaration of September 2014;

(2) the United States Government should continue efforts through the Department of Defense and other agencies to encourage North Atlantic Treaty Organization allies towards meeting the defense spending goals set out at the Wales Summit;

(3) some North Atlantic Treaty Organization allies have already taken positive steps to reverse declines in defense spending and should continue to be supported in those efforts; and

(4) thoughtful and coordinated defense investments by European allies in military capabilities would add deterrence value to the posture of the North Atlantic Treaty Organization against Russian aggression and terrorist organizations and more appropriately balance the share of Atlantic defense spending.

Section 1255 of S. 1376 as reported by the committee states:

SEC. 1255. Additional matters in annual report on military and security developments involving the Russian Federation.

(a) Additional matters.—Subsection (b) of section 1245 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291) is amended—

(1) by redesignating paragraphs (4) through (15) as paragraphs (6) through (17), respectively; and

(2) by inserting after paragraph (3) the following new paragraphs (4) and (5):

"(4) An assessment of the force structure and capabilities of Russian military forces stationed in each of the Arctic, Kaliningrad, and Crimea, including a description of any changes to such force structure or capabilities during the one-year period ending on the date of such report and with a particular emphasis on the anti-access and area denial capabilities of such forces.

"(5) An assessment of Russian military strategy and objectives for the Arctic region.".

(b) Effective date.—The amendments made by subsection (a) shall take effect on the date of the enactment of this Act, and shall apply with respect to reports submitted under section 1245 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 after that date.

Regarding Section 1255, S.Rept. 114-49 states:

Additional matters in annual report on military and security developments involving the Russian Federation (sec. 1255)

The committee recommends a provision that would add a reporting requirement to section 1245 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291) requiring an assessment of the force structure and capabilities of Russian military forces stationed in the Arctic region, Kaliningrad, and Crimea, as well as an assessment of the Russian military strategy in the Arctic region.

The committee is concerned about increased Russian military activity in the Arctic region and notes that Russian activities and apparent ambitions could present challenges to international law, norms, and agreements relating to the Arctic region. (Page 233)

Section 1256 of S. 1376 as reported by the committee states:

SEC. 1256. Report on alternative capabilities to procure and sustain nonstandard rotary wing aircraft historically procured through Rosoboronexport.

(a) Report on assessment of alternative capabilities.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Defense for Acquisition, Technology, and Logistics shall, in consultation with the Chairman of the Joint Chiefs of Staff, submit to the congressional defense committees a report setting forth an assessment, obtained by the Under Secretary for purposes of the report, of the feasibility and advisability of using alternative industrial base capabilities to procure and sustain, with parts and service, nonstandard rotary wing aircraft historically acquired through Rosoboronexport, or nonstandard rotary wing aircraft that are in whole or in part reliant upon Rosoboronexport for continued sustainment, in order to benefit United States national security interests.

(b) Independent assessment.—The assessment obtained for purposes of subsection (a) shall be conducted by a federally funded research and development center (FFRDC), or another appropriate independent entity with expertise in the procurement and sustainment of complex weapon systems, selected by the Under Secretary for purposes of the assessment.

(c) Elements.—The assessment obtained for purposes of subsection (a) shall include the following:

(1) An identification and assessment of international industrial base capabilities, other than Rosoboronexport, to provide one or more of the following:

(A) Means of procuring nonstandard rotary wing aircraft historically procured through Rosoboronexport.

(B) Reliable and timely supply of required and appropriate parts, spares, and consumables of such aircraft.

(C) Certifiable maintenance of such aircraft, including major periodic overhauls, damage repair, and modifications.

(D) Access to required reference data on such aircraft, including technical manuals and service bulletins.

(E) Credible certification of airworthiness of such aircraft through physical inspection, notwithstanding any current administrative requirements to the contrary.

(2) An assessment (including an assessment of associated costs and risks) of alterations to administrative processes of the United States Government that may be required to procure any of the capabilities specified in paragraph (1), including waivers to Department of Defense or Department of State requirements applicable to foreign military sales or alterations to procedures for approval of airworthiness certificates.

(3) An assessment of the potential economic impact to Rosoboronexport of procuring nonstandard rotary wing aircraft described in paragraph (1)(A) through entities other than Rosoboronexport.

(4) An assessment of the risks and benefits of using the entities identified pursuant to paragraph (1)(A) to procure aircraft described in that paragraph.

(5) Such other matters as the Under Secretary considers appropriate.

(d) Use of previous studies.—The entity conducting the assessment for purposes of subsection (a) may use and incorporate information from previous studies on matters appropriate to the assessment.

(e) Form of report.—The report under subsection (a) shall be submitted in unclassified form, but may include a classified annex.

Regarding Section 1256, S.Rept. 114-49 states:

Report on alternative capabilities to procure and sustain nonstandard rotary wing aircraft historically procured through Rosoboronexport (sec. 1256)

The committee recommends a provision that would require an independent assessment directed by the Under Secretary of Defense for Acquisition, Technology, and Logistics in consultation with the Chairman of the Joint Chiefs of Staff to report on the feasibility and advisability of using alternative industrial base capabilities to procure and sustain nonstandard rotary wing aircraft historically acquired through the Russian state corporation Rosoboronexport. The assessment would include an analysis of the economic impact as well as alterations that would be required for waivers of foreign military sales requirements and procedures for approval of airworthiness certificates.

The committee notes that the use of alternative industrial base capability to divest reliance on Rosoboronexport could benefit United States national security interests, deny financial support to the Russian Federation, and could potentially benefit U.S. and Ukrainian commercial interests. (pages 233–234)

Section 1603 of S. 1376 as reported by the committee states:

SEC. 1603. Exception to the prohibition on contracting with Russian suppliers of rocket engines for the evolved expendable launch vehicle program.

Section 1608 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291; 128 Stat. 3626; 10 U.S.C. 2271 note) is amended—

(1) in subsection (a), by striking "subsections (b) and (c)" and inserting "subsections (b), (c), and (d)"; and

(2) by adding at the end the following new subsection:

"(d) Special rule for phase 1A competitive opportunities.—

"(1) IN GENERAL.—For not more than 9 competitive opportunities described in paragraph (2), the Secretary of Defense may award a contract—

"(A) requiring the use of a rocket engine designed or manufactured in the Russian Federation that is eligible for a waiver under subsection (b) or an exception under subsection (c); or

"(B) if a rocket engine described in subparagraph (A) is not available, requiring the use of a rocket engine designed or manufactured in the Russian Federation that is not eligible for such a waiver or exception.

"(2) COMPETITIVE OPPORTUNITIES DESCRIBED.—A competitive opportunity described in this paragraph is—

"(A) an opportunity to compete for a contract for the procurement of property or services for space launch activities under the evolved expendable launch vehicle program; and

"(B) one of the 9 Phase 1A competitive opportunities for fiscal years 2015 through 2017, as specified in the budget justification materials submitted to Congress in support of the budget of the President for fiscal year 2016 (as submitted to Congress under section 1105(a) of title 31, United States Code).".

Regarding Section 1603, S.Rept. 114-49 states:

Exception to the prohibition on contracting with Russian suppliers of rocket engines for the Evolved Expendable Launch Vehicle program (sec. 1603)

The committee recommends a provision that would amend section 1608 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113–291; 128 Stat. 3626; 10 U.S.C. 2271 note) by adding a special rule for Phase 1A competitive opportunities. For not more than nine competitive Phase 1A launches, the special rule would allow the Secretary of Defense to award a contract requiring the use of a rocket engine designed or manufactured in the Russian Federation that is eligible for the existing waiver or exception requirements as specified in the existing statute. If a circumstance arises during the Phase 1A period where a launch provider is awarded a competitive contract and requires a rocket engine unable to meet the waiver or exception

requirements, the provision would allow for the Secretary to waive the waiver or exception. In order to qualify for the new special rule, all engines that meet the waiver or exception of the existing statute must first be used.

The committee notes that for the Phase 1A competitive period, this could result in as few as zero Russian rocket engines or up to nine, depending upon the outcome of the competitions. The committee believes that the continued use of Russian rocket engines represents a threat to our national security and that their use should be minimized to the greatest extent practicable.

National Security Presidential Directive 40 states that Assured Access to Space is ''a requirement for critical national security, homeland security, and civil missions and is defined as a sufficiently robust, responsive, and resilient capability to allow continued space operations, consistent with risk management and affordability. The Secretary of Defense and the Administrator of the National Aeronautics and Space Administration, as appropriate, are responsible for assuring access to space.'' The committee notes that under section 1608, the National Aeronautics and Space Administration (NASA) is not prohibited from procuring launches that utilize rocket engines manufactured or designed in the Russian Federation. The committee also notes that NASA has contracts for numerous launches that rely on Russian rocket engines for the foreseeable future. While the committee does not condone the use of Russian rocket engines for NASA purposes, the committee recognizes that assured access to space can still be met if a national emergency required the use of a NASA procured launch for Department of Defense purposes. (Pages 258–259)

S.Rept. 114-49 also states:

Committee overview

For seven decades, the U.S. military has been the most reliable guarantor of the foundations of international order that American statesmen of both parties helped to establish in the aftermath of World War II. The relative security and prosperity that our nation has enjoyed, and made possible for so many others across the world, has been painstakingly maintained through the deterrence of adversaries, the cooperation with allies and partners, the global leadership of the United States, and the credibility and capability of our Armed Forces.

The committee is concerned that growing threats abroad and continued limitations on defense spending at home are increasingly harming the ability of the United States, and its military, to play an effective leadership role in the world. Indeed, military readiness and capabilities have deteriorated to the point where senior military leaders have warned that we are putting at risk the lives of the men and women who serve in our Armed Forces. There is a growing consensus that we must reverse this damage so that we can respond adequately to a host of disturbing challenges to the international order that adversely impact our national security.

These challenges include:

- In Ukraine, Russia has sought to redraw an international border and annex the territory of another sovereign country through the use of military force.

It continues aggressively to destabilize Ukraine, with troubling implications for security in Europe.

- A terrorist army with tens of thousands of fighters, many holding Western passports, has taken over a vast swath of territory and declared an Islamic State in the heart of the Middle East. Nearly 3,000 U.S. troops have returned to Iraq to combat this threat, with U.S. aircraft flying hundreds of strike missions a month over Iraq and Syria.
- Amid negotiations over its nuclear program, Iran continues to pursue its ambitions to challenge regional order in the Middle East by increasing its development of ballistic missiles, support for terrorism, training and arming of pro-Iranian militant groups, and other malign activities in places such as Iraq, Syria, Lebanon, Gaza, Bahrain, and Yemen.
- Yemen has collapsed, as a Shia insurgency with ties to the Iranian regime has toppled the U.S.-backed government in Sanaa, Al-Qaeda continues to use parts of the country to plan attacks against the West, the U.S. Embassy has been evacuated, and a U.S.-backed coalition of Arab nations has intervened militarily to reverse the gains of the Houthi insurgency and to restore the previous government to power.
- Libya has become a failed state, beset by civil war and a growing presence of transnational terrorist groups, such as al-Qaeda and ISIL, similar to Afghanistan in 2001.
- North Korea, while continuing to develop its nuclear arsenal and ever-more capable ballistic missiles, committed the most destructive cyberattack ever on U.S. territory.
- China is increasingly taking coercive actions to assert expansive territorial claims that unilaterally change the status quo in the South and East China Seas and raise tensions with U.S. allies and partners, all while continuing to expand and modernize its military in ways that challenge U.S. access and freedom of movement in the Western Pacific. (Pages 2–3)

S.Rept. 114-49 also states:

Congressional Defense Review to Prepare for Future Strategic Challenges

For the past 14 years, the United States has been engaged in a long war against terrorist and violent extremist groups. The committee believes that this conflict will persist, at one level or another, across multiple theaters of operation, for some time to come, and that winning this war must be a top priority of the U.S. military and the Department of Defense (DOD).

At the same time, the committee is deeply concerned by the growth of more traditional security threats posed by powerful states, such as China and Russia, and rogue regimes such as Iran and North Korea. States such as these are modernizing their military capabilities, developing advanced technologies that could undermine U.S. military advantages—from precision-guided munitions and advanced sensors, to undersea-warfare and unmanned systems, to offensive cyber and space capabilities—and pursuing strategies that seek to deter the United States

from achieving its national security interests and meeting its commitments to allies and partners.

Secretary of Defense Ashton Carter captured this new military challenge well when he said "for decades, U.S. global power projection has relied on the ships, planes, bases, aircraft carriers, satellite networks, and other advanced capabilities that comprise our military's unrivaled technological edge. But today that superiority is being challenged in unprecedented ways." In short, for the first time in three decades, the United States faces a potential turning point where our nation's long-standing military advantages threaten to be eroded by new shifts in the balance of military power.

Accordingly, over the coming 18 months, the committee plans to conduct a comprehensive review of the roles, capabilities/size of the U.S. Armed Forces and DOD in meeting, and succeeding against, these new security challenges, especially those posed by the growing anti-access/area denial capabilities of U.S. adversaries. This review will utilize open hearings, classified briefings, the Government Accountability Office, the Congressional Research Service, Federally Funded Research and Development Centers, and consultation with former senior defense and military leaders and other national security experts. Building on the series of strategy-focused hearings that the committee has already conducted, the committee will deepen its oversight of military strategy while also delving deeper into intelligence and threat assessments, contingency planning, force structure and posture, joint concept development, domestic and overseas basing and infrastructure, theater and strategic lift requirements, munition quality and quantity, and institutional and personnel reforms. The committee will also review civilian personnel policy, DOD infrastructure, and acquisition policies and practices to bring them more into line with the needs of the future.

Ultimately, the committee intends to review each of the major defense acquisition programs and its related industrial base to determine whether they are sufficient and appropriate to meet developing national security challenges. This review will take nothing for granted and will evaluate each program, both qualitatively and quantitatively, in the broader context of the roles, missions, requirements, and other capabilities of the armed services, as well as emerging technologies that could significantly alter previous assumptions underpinning the current programs of record. The committee's future budgetary decisions will be based on the outcome of this strategic review.

The committee acknowledges that for this review to be successful it will require a sustained commitment of many years and potentially multiple chairmen. The much-heralded "offset strategy" of the 1970s required a tremendous amount of intellectual capital and research and development dollars invested over the course of a decade before capabilities like stealth, precision-guided-munitions, and advanced sensors could be effectively deployed. Nevertheless, it is possible to embark upon a new period of sustained military innovation today if DOD, the military services, and industry can be aligned towards this goal. The committee intends to use all of the resources at its disposal to this end. (Page 214–215)

S.Rept. 114-49 also states:

Countering Russian propaganda

The committee has watched with increasing concern the proliferation and expansion of Russian propaganda not only in Eastern Europe, but also throughout Central and Western Europe to levels not seen since the end of the Cold War. Russian-speaking populations in Eastern Europe in former Soviet Union nations, including North Atlantic Treaty Organization (NATO) allies, are especially vulnerable to propaganda that could be used to create more favorable conditions for future Russian aggression. Moreover, the sophistication and pervasiveness of outlets such as the Russia Today (RT) television network that broadcast in multiple languages in Western European democracies is cause for concern.

The committee notes that Russian propaganda has promoted a false narrative on the nature, scope, and cause of the conflict in Crimea and eastern Ukraine and has unfortunately achieved some success with targeted audiences in obscuring attribution for Russian-driven aggression and disregard for sovereignty, territorial integrity, and international law.

The committee recognizes that propaganda is a critical element of Russia's ''hybrid warfare'' concept. The speed and reach of Russian propaganda and the ambiguity it creates pose a challenge to NATO collective defense and the political consensus upon which it relies.

Therefore, the committee encourages the Secretary of Defense to consult with the Secretary of State with the objective of developing a strategy, including supporting resources, to counter Russian propaganda in Europe. (page 238)

S.Rept. 114-49 also states:

Report on capability of the North Atlantic Treaty Organization to respond to unconventional or hybrid warfare tactics such as used by the Russian Federation in Crimea and Eastern Ukraine

The committee is concerned about the capability of the North Atlantic Treaty Organization (NATO) to respond to unconventional or hybrid warfare tactics such as those used by the Russian Federation in Crimea and eastern Ukraine due to the ambiguous nature of those tactics and the resultant challenges of attribution. As such, the committee directs the Secretary of Defense to submit a report not later than September 1, 2016 to the congressional defense committees on recommendations for improving the alliance's response options, decision-making processes and implementation timelines for addressing the use of unconventional or hybrid warfare tactics such as those used by the Russian Federation. The report should include:

(1) An identification of the unconventional or hybrid tactics the Russian Federation may employ against NATO nations;

(2) A consolidation of tactics identified pursuant to paragraph (1) into a set of possible scenarios to be used to analyze potential response options by NATO;

(3) An assessment of the response options NATO could potentially pursue for each of the scenarios identified pursuant to paragraph (2);

(4) Recommendations to improve response options, decisionmaking processes, and implementation timelines for the scenarios identified pursuant to paragraph (2);

(5) An assessment of implementation by NATO of commitments made at the Wales Summit regarding the Readiness Action Plan;

(6) Recommendations, if any, for exercises or mechanisms to improve the ability of NATO to consult and reach consensus in scenarios relating to the employment of unconventional or hybrid tactics; and

(7) Such other matters as the Secretary considers appropriate. (page 240)

FY2016 DOD Appropriations Act (H.R. 2685/S. 1558)

House

Section 8105 of H.R. 2685 as reported by the House Appropriations Committee (H.Rept. 114-139 of June 5, 2015) states:

Sec. 8105. (a) None of the funds appropriated or otherwise made available by this or any other Act may be used by the Secretary of Defense, or any other official or officer of the Department of Defense, to enter into a contract, memorandum of understanding, or cooperative agreement with, or make a grant to, or provide a loan or loan guarantee to Rosoboronexport or any subsidiary of Rosoboronexport.

(b) The Secretary of Defense may waive the limitation in subsection (a) if the Secretary, in consultation with the Secretary of State and the Director of National Intelligence, determines that it is in the vital national security interest of the United States to do so, and certifies in writing to the congressional defense committees that, to the best of the Secretary's knowledge:

(1) Rosoboronexport has ceased the transfer of lethal military equipment to, and the maintenance of existing lethal military equipment for, the Government of the Syrian Arab Republic;

(2) the armed forces of the Russian Federation have withdrawn from Crimea, other than armed forces present on military bases subject to agreements in force between the Government of the Russian Federation and the Government of Ukraine; and

(3) agents of the Russian Federation have ceased taking active measures to destabilize the control of the Government of Ukraine over eastern Ukraine.

(c) The Inspector General of the Department of Defense shall conduct a review of any action involving Rosoboronexport with respect to a waiver issued by the Secretary of Defense pursuant to subsection (b), and not later than 90 days after the date on which such a waiver is issued by the Secretary of Defense, the Inspector General shall submit to the congressional defense committees a report containing the results of the review conducted with respect to such waiver.

H.Rept. 114-139 states:

> EUROPEAN REASSURANCE INITIATIVE
>
> The Committee supports efforts started in fiscal year 2015 to reassure NATO allies and partners of the continued commitment of the United States to their security and territorial integrity. The Committee recommends $789,300,000 for the European Reassurance Initiative (ERI) to support increased capability, presence, readiness, and responsiveness to deter further destabilization in central and eastern Europe. Efforts include an increased U.S. military presence in Europe, additional bilateral and multilateral exercises and training opportunities with allies and partners, improved infrastructure to allow for greater responsiveness, enhanced prepositioning of equipment in Europe, and intensified efforts to build partner capacity for new NATO members and other partners.
>
> This funding is provided as requested in the fiscal year 2016 budget request in the military personnel and operation and maintenance accounts at the budget activity and sub-activity group level of detail. The Committee again directs the Secretary of Defense to request any required fiscal year 2017 funding within the existing military personnel and operation and maintenance accounts as part of the fiscal year 2017 budget request. (Pages 317–318)

Senate

Section 8105 of S. 1558 as reported by the Senate Appropriations Committee (S.Rept. 114-63 of June 11, 2015) states:

> Sec. 8105. (a) None of the funds appropriated or otherwise made available by this or any other Act may be used by the Secretary of Defense, or any other official or officer of the Department of Defense, to enter into a contract, memorandum of understanding, or cooperative agreement with, or make a grant to, or provide a loan or loan guarantee to Rosoboronexport or any subsidiary of Rosoboronexport.
>
> (b) The Secretary of Defense may waive the limitation in subsection (a) if the Secretary, in consultation with the Secretary of State and the Director of National Intelligence, determines that it is in the vital national security interest of the United States to do so, and certifies in writing to the congressional defense committees that, to the best of the Secretary's knowledge:
>
> (1) Rosoboronexport has ceased the transfer of lethal military equipment to, and the maintenance of existing lethal military equipment for, the Government of the Syrian Arab Republic;
>
> (2) The armed forces of the Russian Federation have withdrawn from Crimea, other than armed forces present on military bases subject to agreements in force between the Government of the Russian Federation and the Government of Ukraine; and
>
> (3) Agents of the Russian Federation have ceased taking active measures to destabilize the control of the Government of Ukraine over eastern Ukraine.

(c) The Inspector General of the Department of Defense shall conduct a review of any action involving Rosoboronexport with respect to a waiver issued by the Secretary of Defense pursuant to subsection (b), and not later than 90 days after the date on which such a waiver is issued by the Secretary of Defense, the Inspector General shall submit to the congressional defense committees a report containing the results of the review conducted with respect to such waiver.

Author Contact Information

Ronald O'Rourke
Specialist in Naval Affairs
rorourke@crs.loc.gov, 7-7610

B. UNDERSTANDING HYBRID WARFARE AND GRAY ZONE THREATS

COMMENTARY

by
Douglas C. Lovelace, Jr.

Section B of this volume presents three documents to provide a palpable introduction to the concept of hybrid warfare. The comprehensive report on "Hybrid Warfare" by the Joint Special Operations University (JSOU) uses a historical analysis to arrive at an overarching description of hybrid warfare and then tests that decription against actual case studies. Major Tim McCulloh, author of the first article within this report, "The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the 'Hybrid Threat' New?," presents a "unifying logic to hybrid behavior" expressed in seven "principles." His first principle is that "a hybrid force's composition, capabilities, and effects are unique to the force's own specific context." Of course, that is a correct, if not obvious, statement. The blending of the varying types of coercive capabilities that a hybrid force will seek to achieve depends on the nature of the adversary it seeks to overcome coupled with the resources available to the hybrid force and the nature of the area of operations and its population.

Thus, an astute military strategist should be able to predict, at least in general terms, how a potential hybrid force might be composed and structured, as well as what tactics it might employ. But, of course, the calculus on both sides is dynamic. That is, to the extent that a hybrid threat is able to understand how an adversary might prepare to thwart it, there is also a greater likelihood that the hybrid threat will make itself something different, at least to the extent that available resources and the nature of the operational area afford choices to the hybrid threat.

Major McCulloh's second point is that "there exists a specific ideology within [each] hybrid force that creates an internal narrative to [*sic*] the organization." One can accept this principle if the definition of "ideology" is sufficiently broad. The principle is easily understood where ideology refers to a belief system about the specific role tenets of a particular religion should play in governing populations. However, for the principle to be generally valid, greed and profit motives, revenge, ethnic and religious hatred, authoritarianism, and the like must also be defined as ideologies.

The Major's third principle is that "a hybrid force perceives an existential threat by a potential adversary." For the cases studied in the JSOU report, this principle holds true. But more must be said. In some cases, hybrid threats can be opportunistic, rather than survivalist. In those cases, the calculus is more of a cost/benefit analysis than a survival plan. Vladimir Putin's aggression in Ukraine and, arguably, his aggression in Georgia before it, were hybrid, Gray Zone, actions not based on the survival of Russia. Similarly,

China's aggressions in the East China Sea and South China Sea are hegemonic, and not matters of survival. The same can be said for many of Iran's actions.

The fourth principle Major McCulloh proposes is that "a capability overmatch between the hybrid force and a potential adversary exists." This point seems intuitively obvious but is actually not quite accurate. It could be better stated that "in hybrid war there is a capability asymmetry between adversaries." A belligerent could have conventional military superiority over a hybrid adversary but be so lacking in other capabilities as to suffer a power deficiency relative to the hybrid adversary. In fact the authors of the JSOU report make that very point in their case study analyses.

Major McCulloh's fifth principle—that "a hybrid force contains both conventional and unconventional elements—" is a fundamental aspect of his definition of a hybrid force, but is not a necessary descriptor of hybrid forces in general. A hybrid force could contain no conventional forces; i.e., tanks, bombers, warships, etc., but still be hybrid in that it contains irregular forces, mercenaries, propagandists, criminals, and unconventional weapons, all combined to form a hybrid force.

The sixth principle of a hybrid force advanced in the JSOU report is that "hybrid organizations rely on inherently defensive type operations . . . to defend [their] existence." Again, while this principle holds true for the type of hybrid forces the report's authors contemplate, it is not true in broad, general terms, as suggested above. Russian actions in Ukraine and China's moves in its near abroad are anything but defensive. The authors of the JSOU report appear to recognize the limited application of this principle when they acknowledge that defensive operations can have offensive components.

The final principle Major McCulloh sets forth is that "hybrid organizations use attritional tactics . . . to continually whittle away the adversary's forces and his will to use them." While this principle holds sufficiently true to qualify as a principle, there are significant exceptions to it. Hybrid threats employing terrorism as part of their armory, for example, often seek a debilitating master stroke that will convince an adversary to accede to the hybrid force's demands.

The second document in Section B is a somewhat dated but still very useful Government Accountability Office (GAO) report entitled "Hybrid Warfare." The U.S. Congress astutely asked the GAO to examine whether the Department of Defense (DOD) has defined hybrid warfare and how hybrid warfare differs from other types of warfare. Congress also asked the GAO to determine the extent to which the DOD considers the implications of hybrid warfare in its strategic planning documents. Interestingly, the GAO found that nowhere within any DOD publication is hybrid warfare defined. That remains the case today. Perhaps more importantly, no agency within the DOD intends to define hybrid warfare formally, asserting that hybrid warfare is nothing new and that it does not suggest any new approaches to defending and promoting U.S. national security interests.

The DOD's belief that the increased appearance of hybrid warfare within the evolving international security environment does not require acceptance of the term within its doctrinal lexicon suggests that the department will continue to be surprised by hybrid enemies and unprepared to counter them effectively. Typically, the DOD deals with a new threat by identifying it, defining it, developing a concept or concepts for countering it, converting the concepts into doctrine, and then applying the most effective and

efficient combination of leadership, organizational change, equipment, personnel, and training to counter the threat. Putting the chain of events in motion requires the threshold requirement that the threat be identified and defined. It is troubling that the DOD, constrained by its residual Cold War military forces, cannot come to grips with such an obviously emerging threat.

The final document of Section B is a March 10, 2015, U.S. Army Special Operations Command "White Paper" on "SOF Support to Political Warfare." It embraces the Clausewitzian axiom that war is the continuation of politics by other means and focuses on Russian hybrid warfare, China's concept of "unrestricted warfare" and Iran's "asymmetric warfare." For all practical purposes, unsresticted warfare and asymmetric warfare can be considered versions of hybrid warfare. The White Paper does a good job of describing the emerging international security environment from an operational perspective, projects a future operating environment, and explains what the environment portends for the U.S. military. Unsurprisingly, the White Paper focuses on contributions Special Operations Forces (SOF) can make to protecting and promoting U.S. national security interests, in the increasingly unpredictable and volatile international security environment.

Significantly, the White Paper discusses the application of military power as but one instrument of U.S. national power and considers the need for synergistic employment of diplomatic, economic, and informational elements of national power as well. The Paper defines political warfare as "a strategy suited to achieve U.S. national objectives through reduced visibility in the international geo-political environment, without committing large military forces." That is, it suggests a hybrid warfare approach suitable for employment by the United States. The most salient and powerful statement made in the paper is that "rather than a binary opposition between 'war' and 'peace,' the conduct of international relations is characterized by continuously evolving combinations of collaboration, conciliation, confrontation, and conflict. As such, during times of interstate 'peace,' the U.S. government must still confront adversaries aggressively and conclusively through all means of national power." This observation should serve as the guiding principle for U.S. national security planning and operations during the current era of hybrid warfare and Gray Zone threats.

DOCUMENT NO. 2

HYBRID WARFARE

JOINT SPECIAL OPERATIONS UNIVERSITY
JSOU

JSOU Report 13-4
The JSOU Press
MacDill Air Force Base, Florida
2013

This monograph and other JSOU publications can be found at https://jsou.socom.mil. Click on Publications. Comments about this publication are invited and should be forwarded to Director, Strategic Studies Department, Joint Special Operations University, 7701 Tampa Point Blvd., MacDill AFB, FL 33621.

****

The JSOU Strategic Studies Department is currently accepting written works relevant to special operations for potential publication. For more information please contact the JSOU Research Director at jsou_research@socom.mil. Thank you for your interest in the JSOU Press.

****

This work was cleared for public release; distribution is unlimited.

ISBN: 978-1-933749-77-8

The views expressed in this publication are entirely those of the authors and do not necessarily reflect the views, policy or position of the United States Government, Department of Defense, United States Special Operations Command, or the Joint Special Operations University.

Foreword

Major Tim McCulloh and Major Rick Johnson's combined contributions to this monograph on Hybrid Warfare benefit from a combination of both an overarching theory as well as an operational perspective. The combination of the works into a single manuscript provides a synergy of the two perspectives. While the idea of hybrid warfare is not new, the authors

together provide a clarity and utility which presents a relevant contextual narrative of the space between conventional conflicts and realm of irregular warfare.

Major McCulloh's contribution in the first section entitled *The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the 'Hybrid Threat' New?* lays the theoretical basis to bring a definition of Hybrid Warfare into focus while addressing the pertinent question of its historical origin. The theory presented uses historical trends, illustrated through two case studies, to postulate a set of principles to provide a unifying logic to hybrid behavior. In the first study, Major McCulloh examines the Israel-Hezbollah war of 2006. Within this case study, Major McCulloh's six principles of hybrid warfare are defined as: (1) a hybrid force's composition, capabilities, and effects are unique to the forces context; (2) each hybrid force has a specific ideology that creates an internal narrative to the organization; (3) a hybrid force always perceives an existential threat to its survival; (4) in hybrid war there is a capability overmatch between adversaries; (5) a hybrid force contains both conventional and unconventional components; and (6) hybrid forces seek to use defensive operations. To test the theory, Major McCulloh then examines the Soviet partisan network on the Eastern Front from 1941–1945. With the two case studies examined under the same theoretical framework, Major McCulloh asserts that the framework can be used as tool for anticipating emergent hybrid organizations while demonstrating historical continuity.

With a theoretical underpinning having been argued by Major McCulloh, the strategic studies question of "so what?" is addressed at the operational level by Major Johnson. In Major Johnson's section entitled *Operational Approaches to Hybrid Warfare,* the author uses historical examples and case studies to form a basis for approaching hybrid threats through a lens of U.S. oriented operational art. Major Johnson uses case studies of U.S. efforts in Vietnam and Iraq to illuminate operational approaches to defeating hybrid threats. Much like Major McCulloh, Major Johnson utilizes the Israel-Hezbollah conflict of 2006 as a starting point, contextualizes hybrid warfare vis-à-vis other mixed forms of warfare, addresses the nature of operational art, and then delves backward to find validation of the author's propositions. In examining the case of Vietnam, Major Johnson examines the synergistic effects of Communist organization, strategy, and operational flexibility in depth which serves to highlight the concurrent political and military efforts used by the Vietcong and North Vietnamese. In the Iraq case study, Major Johnson examines a profoundly complex and varied adversary juxtaposed to the organizational harmony presented in the Vietnam case study. Major Johnson examines two radically different conflicts and develops three "imperatives" for operational art in hybrid warfare: (1) an operational approach must disrupt the logic of the forms of conflict the hybrid threat employs; (2) tactical success and strategic aims must be developed within the same context which gave rise to the hybrid threat and; (3) a successful approach should avoid prescriptive measures across time and space.

Many may argue that the concept is not needed or is redundant to other definitions of mixed forms of warfare, or offers nothing unique. However, in this case the authors do contribute to the understanding of warfare as a spectrum of conflict rather than a dichotomy of black and white alternatives. This gray area is sorely needed in the complex and multifaceted conflict environment prevalent in the world today.

Kenneth H. Poole, Ed.D.
Director, JSOU Strategic Studies Department

About the Authors

Major Timothy B. McCulloh began his Army service in 1993 as a Combat Medical Specialist in the Army National Guard. In 1998, he graduated from Cornell College and was commissioned as an Army Officer through the University of Iowa Reserve Officer Training Program. Major McCulloh was assigned to the 101st Airborne Division (Air Assault) at Fort Campbell, Kentucky where he served as a Platoon Leader, Assistant Battalion Operations Officer, and Battalion Personnel Officer in the 3rd Brigade Combat Team (187th Infantry Regiment). In November 2001 he deployed to Afghanistan as a Rifle Platoon Leader in support of Operation Enduring Freedom.

Following his deployment to Afghanistan, Major McCulloh served as an Infantry Basic Training Company Commander and completed the Infantry Captain's Career Course at Fort Benning, Georgia. Major McCulloh was then assigned to the 172nd Stryker Brigade Combat Team at Fort Wainwright, Alaska as an Assistant Brigade Operations Officer, Headquarters Company Commander, Stryker Company Commander, and Brigade Plans Chief. During this time, he deployed in support of Operation Iraqi Freedom from July 2005 to December 2006 in Mosul and later in Baghdad, Iraq as the first unit in the "Surge."

Major McCulloh then served as a Plans Officer and a Plans Branch Chief in U.S. Army Central (ARCENT) at Fort McPherson, Georgia. During this time he deployed in support of Multinational Forces-Iraq, U.S. Central Command, U.S. Special Operations Command, and multiple other commands throughout the Middle East conducting Contingency Planning, Operational Planning, and Theater Security Cooperation Activities.

After ARCENT, Major McCulloh attended and graduated from the U.S. Army Command and General Staff College. He remained at Fort Leavenworth to attend the School of Advanced Military Studies during which he completed the monograph upon which this publication is based.

Major McCulloh holds Bachelor of Arts degrees in Biology, Psychology, and Origins of Behavior from Cornell College; a master's degree in Business Administration from Touro University; and a Master of Military Arts and Science from the School of Advanced Military Studies. Major McCulloh is currently assigned to the 101st Airborne Division Headquarters (Air Assault) where he is deployed as the Task Force Executive Officer in Bagram, Afghanistan.

Major Richard Johnson began his Army service in 1999 upon graduation from the United States Military Academy with a commission in the Field Artillery. After graduation from the Field Artillery Officer's Basic Course and Ranger School, Rick was assigned to the 1st Armored Division in Idar-Oberstein, Germany where he served as a Platoon Leader, Battery Operations Officer and Battalion Fire Direction Officer with service in West Baghdad during Operation Iraqi Freedom.

After completing the Field Artillery Captain's Career Course, Major Johnson was assigned to the 82d Airborne Division at Fort Bragg, North Carolina where he served as a Battalion Fire Support Officer, Assistant Battalion Operations Officer, and Battery Commander in the 3rd Brigade Combat Team. During this time, he deployed to New

Orleans in support of Hurricane Katrina recovery efforts and Tikrit for Operation Iraqi Freedom 2006–2008. He continued serving the 3rd Brigade Combat Team as the Headquarters and Headquarters Company Commander and the Assistant Brigade Fire Support Officer in another deployment to East Baghdad for Operation Iraqi Freedom 2008–2009.

Upon successful completion of those duties, Major Johnson attended and graduated from the U.S. Army Command and General Staff College. He was selected for the Art of War Scholars program, and completed his thesis "The Biggest Stick: The Employment of Artillery Units in Counterinsurgency," which was published by the Combat Studies Institute in 2012. He remained at Fort Leavenworth to attend the School of Advanced Military Studies, during which he completed the monograph upon which this publication is based.

Major Johnson holds a Bachelor of Science in Systems Engineering from the United States Military Academy; a Master's Degree in Management and Leadership from Webster University; a Master of Military Arts and Science from the Command and General Staff College; and a Master of Military Arts and Science from the School of Advanced Military Studies. Major Johnson is currently assigned to the 82d Airborne Division where he serves as a Plans Officer.

The Inadequacy of Definition and the Utility of a Theory of Hybrid Conflict: Is the "Hybrid Threat" New?

by Major Timothy B. McCulloh

> The most likely security threats that Army forces will encounter are best described as hybrid threats.[1]

1. Introduction

This monograph will attempt to answer the question of why hybrid actors, or hybrid threats, function in the specific manner that they do. In doing so, it proposes a theory of hybrid warfare which will set forth a series of principles observable in historical trends that provide a unifying logic to hybrid behavior. As this monograph outlines a theory of hybrid warfare, it explores the contemporary relevance of hybrid military organizations, the existing body of literature referring to hybrid threats, and historical examples of hybrid threats as they exemplify the proposed theoretical principles. This monograph will then conclude with a discussion of the proposed theory and the potential applications of a theory of hybrid warfare within the U.S. military.

The U.S. military is an organization which exists to support and defend the Constitution of the U.S. against all enemies, foreign and domestic.[2] Within this broad charter, there exists a requirement to confront real and potential adversaries. In order to do this, the U.S. must identify and understand likely threats in order to best prepare for this confrontation. Typically, across the spectrum of armed conflict contemporary threats are placed in one of three different categories—conventional, hybrid, and unconventional.[3] Military planning documents and strategies further indicate that hybrid threats will likely define the contemporary operating environment as the preponderance in number and type of security threats that will be faced in the future; however, definitions of hybrid threats and hybrid warfare vary and contradict each other.[4] This variance and contradiction stymie the ability of military planners to prepare specifically to meet this challenge. Thus, this monograph will seek to clarify the discussion of hybrid organizations and hybrid warfare through the formulation of a theory suggesting principles of hybrid warfare.

In order to establish parameters for the following theoretical discussion and to avoid confusion during the following discussion, this monograph defines certain terms regarding a theory of hybrid warfare. Throughout this paper, the terms regular force and conventional force will be used interchangeably to define military organizations whose behavior conforms to national or international laws, rules, norms, or customs, and whose weapon systems and equipment conform to a commonly accepted standard

---

[1] Headquarters, Department of the Army, *Army Doctrinal Publication 3-0: Unified Land Operations* (Washington, DC: Department of the Army, 2011), 4.

[2] *Oath of Office*, Title 10, U.S. Code; Act of 5 May 1960.

[3] 2010 Quadrennial Defense Review Report, February 2010, 8.

[4] *Hybrid Warfare*, Global Accountability Office, 10 September 2010. This report was initiated at Congressional request to clarify the multiple, conflicting Defense Service definitions, and descriptions of hybrid war, hybrid warfare, and hybrid threats. The 29 page study's official finding was that the existing descriptions of hybrid war were sufficient to the needs of each service and that in the absence of a solidly quantifiably need for a definition that each service be allowed to continue in this manner.

of capabilities.[5] The terms irregular force or unconventional force involve a military type organization that does not conform to commonly accepted standards in either equipment or behavior.[6] This paper discusses the ample definitions of a hybrid force during the literature review of this paper. However, for the purposes of initiating the discussion of hybrid warfare, a hybrid force is a military organization that employs a combination of conventional and unconventional organizations, equipment, and techniques in a unique environment designed to achieve synergistic strategic effects.[7] This definition relies on previous research and discussions by hybrid theorists on hybrid warfare as useful starting points for thinking about hybrid warfare within the spectrum of modern conflicts so that this monograph can add to the working knowledge of hybrid warfare within the defense community.

Certain observations can be made from this brief, albeit broad, definition of hybrid warfare. A hybrid threat uniquely focuses on organizational capability and generally attempts to gain an asymmetrical advantage over purely conventional opponents within a specific environment. This advantage not only asserts itself in the realm of pure military force, but also in a more holistic manner across all the elements of national power including diplomatic, informational, military, economic, financial, intelligence, and law enforcement/legal. The advantage generates the effect of transitioning the rules of the battlefield from those of a conventional fight to those realms of a hybrid's choosing—primarily in the categories of tempo, depth, and intensity. As a result, a weaker military opponent can stand against a stronger one for an indefinite period and continue to generate effects that a more conventional opponent could not generate in the same situation. This hybrid capability poses significant difficulties for large conventional military organizations such as the U.S. military because these large conventional structures are oriented primarily on symmetrical type adversaries, or in the lesser case asymmetrical type adversaries, but never on an efficient combination of the two. Thoroughly understanding this capability can offer insight into methods of understanding and predicting hybrid organizations.

Historical examples of hybrid type warfare reach back to antiquity, even though the term hybrid threat is relatively recent.[8] In ancient Rome, a hybrid force of criminal bandits, regular soldiers, and unregulated fighters employed tactics ranging from that of fixed battle, roadside ambush, and the employment of stolen siege engines against Vespasian's Roman Legions during the Jewish Rebellion of 66 AD.[9] In the Peninsular War of 1806, a hybrid force of Spanish guerillas combined with regular British and

[5] Retrieved from http://www.merriam-webster.com/netdict.htm on 5 April 2012. To further explain the definition of conventional military forces we will include the use of conventional weapons platforms such as tanks, jet fighters, and/or soldiers. This idea of conventional military forces emerged from the Treaty of Westphalia in 1648. This definition describes both form and function.

[6] Retrieved from http://www.merriam-webster.com/netdict.htm on 5 April 2012. This definition will include the concepts of guerilla warfare, asymmetric insurgencies, and unregulated militant forces—all of which will often use low tech weapon systems.

[7] Within this monograph, hybrid organizations are those that engage in hybrid warfare and hybrid threats are hybrid organizations viewed as an adversary. Holistically these terms will be used somewhat interchangeably as they focus on the core concept of hybridity.

[8] As discussed in the literature review, the term "hybrid threat" emerged in U.S. Defense circles following the 2006 Israel-Lebanese Hezbollah War.

[9] Fulvio Poli: *An Asymmetrical Symmetry: How Convention Has Become Innovative Military Thought* (master's thesis, U.S. Army War College, 2010), 2.

Portuguese forces to generate decisive military effects on Napoleon's Grand Armee.[10] During World War II, the Soviet Army on the Eastern Front integrated and synchronized an ill-equipped irregular force with its conventional military forces in order to generate multiple hybrid type effects from 1941 to 1945.[11] During the Vietnam War, the People's Army of Vietnam—the North Vietnamese Regular Army—synchronized its operations with the Viet Cong, an irregular force, in order to sustain a lengthy conflict against the superior conventional forces of two separate First World nations: France and the U.S.[12] The non-state actor in the 2006 Israel-Hezbollah War, Lebanese Hezbollah, combined the aspects of conventional and unconventional war to fight against the premier conventional military power in the Middle East, the Israeli Defense Forces.[13] In each of these historical cases, trends emerge which, arguably, suggest why and how hybrid forces exist, enabling observers and analysts to anticipate the manifestation of hybrid threats in the future.

Regardless of the plentitude of historical examples, a persistent obstacle to understanding the hybrid threat has been a seeming inability to classify what a hybrid threat is and why a hybrid threat coalesces in the first place. The conflicting definitions for this age-old construct have stymied the ability of military theorists and planners to properly envision a common set of hybrid threat motivations and potential actions.[14] Fundamentally, the problem is the gap that exists between the cognitive logic of "definition" and the uniqueness of each context in which "hybrid" manifests itself. No definition can be adequate to multiple contexts that differ in time, space, and logic. This indicates the need for a theory suggesting principles that shed light on the nature and manifestation of hybrid organizations in hybrid conflicts.

This problem of the shortcomings in current thinking about hybrid threats is particularly relevant now in a time of emerging non-state actors and changing state actor dynamics in the Middle East, Africa, and the Pacific. The exponential increases in the availability of information and communication technology and the proliferation of military tactics and weaponry enhance an already strong tendency for Western militaries to substitute information for understanding as well as identify technical solutions to discrete military problems. So this dearth of insight into the nature and potentialities of hybrid conflict becomes even more problematic and dangerous. General George Casey, former Chief of Staff of the Army, highlighted the importance to the U.S. military of understanding hybrid threats when he stated that in the future the U.S. Army must, "prevail in protracted counterinsurgency campaigns; engage to help other nations build capacity and assure friends and allies; support civil authorities at home and abroad; [and] deter and defeat hybrid threats and hostile state actors."[15] Casey's comment was

[10] Phillipe Gennequin, *The Centurions versus The Hydra: French Counterinsurgency in The Peninsular War (1808–1812)* (master's thesis, U.S. Army Command and General Staff College, 2011), 10.

[11] Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), 20.

[12] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 4.

[13] Matthews 2008, 20.

[14] This typically leads to the dismissal or irrelevance of certain elements in a conflict which may actually have an enormous effect—but don't fit into a definition or understanding.

[15] George W. Casey, *The Army of the 21st Century*. Washington, DC: Army Magazine 59 (10), October 2009.

reinforced by the February 2011 version of the U.S. Army's *Field Manual 3.0: Operations* which states:

> The future operational environment will be characterized by hybrid threats: combinations of regular, irregular, terrorist, and criminal groups who decentralize and syndicate against us and who possess capabilities previously monopolized by nation states. These hybrid threats create a more competitive security environment, and it is for these threats we must prepare.[16]

As a result, from the Army Chief of Staff's broad mandate to deter and defeat hybrid threats came the slightly more refined U.S. Army doctrinal response in the Unified Land Operations manual to use varying techniques to meet the different aspects of the hybrid threat. Specifically, the doctrine advises the utilization of "wide area security techniques in population-centric Counter-Insurgency operations [to] confront the unconventional portion of the Hybrid Threat, while [using] combined arms maneuver techniques [to] confront and defeat the conventional portions of the Hybrid Threat."[17] Although this doctrinal approach offers a way of responding to hybrid threats, this prescription does not facilitate any understanding of the nature of the threat or a reference for anticipating contextually unique hybrid organizations; only a theoretical approach will enable this understanding and provide the potential for a relevant response. Therefore, in order to enable a more effective, useful method of responding to this identified threat, this monograph proposes a theory of hybrid warfare.

The comprehensive analysis of historical examples of hybrid conflicts indicates that certain enduring principles of hybrid organizations and hybrid warfare exist. For example, under close observation, repetitive patterns of institutional motivation and tactical application emerge. Elucidation of these repetitive patterns may then offer insight into the underlying logic in a system of hybrid warfare and allow for the formulation of a theory. Such theory, then, could explain the logic of these repetitive patterns, and in doing so enable political and military practitioners to anticipate the manifestation and nature of future hybrid behaviors.

Historical analysis taken with military professionals' and analysts' predictions indicate that hybrid organizations will likely comprise the preponderance of future challenges the U.S. military will face. Therefore, developing a theory of hybrid warfare and an understanding of the components of the hybrid threat will facilitate the training and development of future strategies against these potential threats—from both the conventional and unconventional viewpoint of military force.[18] Understanding how a hybrid military force would likely form and operate in a given environment will offer clear insight into the effectiveness of elements of this strategy. This understanding could then enable the internal optimization of the U.S. military regular and Special Operations Forces (SOF) in terms of equipping and training. A theory would also assist in both the strategic and operational application of military force by the U.S. government and in the refined application of operational art by military leaders against these potential hybrid threats in context.

---

[16] Headquarters, Department of the Army, *Army Field Manual 3-0: Operations* (Washington, DC: Department of the Army, 2011), 14.

[17] ADP 3-0, 2011, 4.

[18] Hoffman 2007, 1-72.

The Lack of Consensual Understanding: A Review of Existing Hybrid Warfare Thinking and Doctrine

A watershed moment came in the *2006 Quadrennial Defense Review* (QDR) when its authors formally recognized the existence of hybrid type threat—the ideas represented in the volume constituted a paradigm shift. This newly emergent thinking was closely following by Frank Hoffman's work on hybrid organizations. Although Western defense establishments—primarily in the U.S., the United Kingdom, and Israel—recognized both of these conceptual events, their thoughts did not represent a consensus in understanding. They assigned many definitions to hybrid scenarios, and provided as many descriptions of them, but each scenario was uniquely tied to both the perspective of the author and the specific milieu of the hybrid organization. As a result, no one single definition or description could be universally applied, or was universally relevant, to any and all potential hybrid scenarios; each scenario required some manipulation in order to fit the model. This lack of consensus and understanding constrained the ability of military professionals in the application of operational art in hybrid situations. This review highlights the evolution and the breadth of the discussion of hybrid warfare to propose a theory that enables the required understanding.

A review of the literature that addresses the fusion of conventional and unconventional warfare and the emergence of the idea of hybrid warfare begin to present principles that can inform a theory of hybrid war. Perhaps one of the useful ways to discuss this emergent theory is to capture it as a point on the evolutionary spectrum of theories of warfare. Based on literature as diverse as western military theory, historical narratives, and national policy statements, this monograph defines war as an organized conflict carried on between armed states, nations, or other parties over a certain period in order achieve a desired political/ideological end state.[19] According to existing theories of modern warfare, war can then be broken into the categories of conventional and unconventional warfare. Historically, theorists may then further analyze warfare as an evolutionary process not only defined by both technology and the employment of forces, but also by social pressures. The dual understanding of warfare as both an evolutionary process and as an activity with many forms sets the stage for greater understanding of hybrid warfare as a sum of many evolving parts whose optimized synergy makes hybrid organizations much more than this sum total of form.

This review presents the existing literature focused on hybrid warfare as it developed chronologically in order to demonstrate the steady evolution of the accepted ideas about modern warfare. Following a discussion of existing military theory relevant to thinking about hybrid organizations in relation to war, the monograph will examine existing military doctrine that has emerged because of the hybrid warfare dialogue. This close examination of the evolution of the existing thinking and the resultant military doctrine relevant to hybrid conflict will serve to highlight how the idea and the premise of application work together. It will also identify potential gaps between the theory and doctrine that warrant further investigation.

A useful starting point on this evolutionary analysis is the generational theory of modern warfare which has been proposed by military theorist Dr. Thomas X. Hammes—a

[19] Retrieved from http://www.merriam-webster.com/netdict.htm on 5 April 2012.

retired Marine colonel—in his book, *The Sling and the Stone: On War in the 21st Century*.[20] Generally, the generational war concept hinges on transformational military technology and its tactical, strategic, and social effects in a wartime setting. Hammes argued that the first generation of modern warfare was a nation-state dominated activity that used the tactics of line and column in close order battle that relied on the technological advantage of rifle and machine gun, prominent primarily in the 18th and early 19th century.[21] Thus, the generations of warfare construct began with the establishment of the Treaty of Westphalia that legitimized the inherent rights of nations to maintain and use military force, thereby essentially discriminating between state and non-state actors.[22] The second generation of warfare built upon the first by utilizing the tactics of linear fire and movement with a focus on indirect fire via artillery that was prominent in the mid-to-late 19th century and early 20th century.[23]

Thomas Hammes characterized the third generation of warfare as an emphasis on the tactics of speed, maneuver, and depth to collapse enemy forces by attacking their rear areas, both military and civilian, with the addition of military air forces. This form of warfare was prominent during the 20th century.[24] Finally, Hammes proposed a fourth generation of warfare which emerged in the mid to late 20th century where state and non-state actors used influencing tactics in addition to military tactics to offset technological capabilities.[25] In this fourth generation of warfare, the ideas of guerilla warfare, insurgency, people's war, and the long war fit to describe a mode of warfare where conventional military advantages offset by unconventional means of warfare are coupled with some unifying thought process that establishes the desired military/political end state. Actors in fourth generation warfare use military influencing operations and strategic communications in conjunction with the unconventional methods to both prolong the conflict and attrite the conventional force's political and military support base. As a relevant contribution to theories of modern warfare, Dr. Hammes made a highly useful contribution to theories of modern warfare in that he established commonly accepted ideas regarding the likely type of warfare that occurred in a certain timeframe and identified the logic of combination in the evolution of modern war.

[20] Thomas X. Hammes, *The Sling and the Stone: On War, in the 21st Century* (St. Paul, MN: MBI Publishing, 2004), 1-321. In no way does Dr. Hammes literature state that the generations of modern warfare that he observes are the first and only examples of the types of warfare that occur. Rather, he attempts to identify the preponderant trends in warfare. For example, guerilla warfare and information warfare existed millennia ago, but were not the preponderant forms or combinations of modern warfare until a certain time in his generational model.

[21] A good example of first generation warfare is that of the Napoleonic Wars.

[22] The historical idea of orderly battle predates the modern timeframe extending back into ancient times with the use of loosely organized armed parties clashing together, followed by the evolving use of the phalanx, sea power, animal domestication, and war machines such as siege engines. Hammes generational narrative best describes modern warfare following the Treaty of Westphalia and using all organizational and tactical precursors. In 4th Generation Warfare, Hammes highlights the loss of a state actor's monopoly on the organized use of force/violence. This generational construct is heavily influenced by the military theories of Antoine Jomini and Carl von Clausewitz following Napoleon Bonaparte's campaigns at the turn of the 18th century.

[23] An example of second generation warfare is World War I.

[24] Examples of third generation warfare are World War II and the Korean War.

[25] Examples of fourth generation warfare are Vietnam, the Iraq War (2003–2011), and the War in Afghanistan (2001).

Mr. Thomas Huber also contributed to this conceptual discussion when he coined the phrase "compound warfare" in his discussion of hybrid-like conflict in his book *Compound Warfare: That Fatal Knot*.[26] He defined compound war simply as the simultaneous use of conventional and unconventional forces.[27] Under this rubric, actors use two types of forces separately under a unifying leadership structure to produce complementary advantages. In this construct, regular forces gain tactical and operational benefits from the intelligence, counterintelligence, speed, logistics support, and defensive nature of irregular forces. In turn, irregular forces reap the benefits of regular force strategic intelligence assets, military logistics structure, and the operational pressure of conventional force operations that force an enemy to operate in a consolidated manner. In essence, the idea of compound warfare builds upon the fourth generation warfare construct to highlight the effectiveness of unconventional forces and to emphasize the complementary nature of regular and irregular forces when they are used in conjunction with each other.[28] However, this idea exists in contrast to the idea of hybrid warfare—which includes conventional, unconventional, criminal, and terrorist aspects. As such, compound warfare exists as a precursor to current thoughts on hybrid warfare and is qualitatively different from hybrid warfare.

The U.S. Department of Defense incorporated the concepts of fourth generation warfare and compound warfare in the 2006 QDR.[29] The 2006 QDR espoused the threat categories of irregular, traditional (conventional), catastrophic (high-end/mass destruction), and disruptive (criminal/terrorist) challenges in contrasting the likelihood and impact of potential threats to the U.S. A quad chart listed the threat categories in terms of frequency and catastrophic effect, enabling a level of prediction regarding enemy threats for the U.S. military. This separate identification of threat elements reflected the idea of compound warfare in which different types of forces could coexist and complement each other on the future battlefield, but it also implied the idea that these categories could hypothetically blur and even fuse together.[30] In doing so, the 2006 QDR opened the door to a spectrum of war that required military planners to think about mixed forces in complex environments—an explicit change from Cold War and Peace Dividend military policies that had laid the essential groundwork for the recognition of hybrid war as a fusion of capabilities. In terms of U.S. defense theories, this action represented a paradigm shift from the Cold War policies that oriented on large scale, symmetrical, state actor threats and Peace Dividend policies that projected limited scope asymmetric threats. In doing so, the Department of Defense formally began a dialogue that would eventually lead to theorizations about hybrid warfare.

---

[26] Thomas Huber, "Compound Warfare: A Conceptual Framework," in *Compound Warfare: That Fatal Knot*, ed. Thomas M. Huber (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2002) 1-317.

[27] Ibid., 10.

[28] Ibid., 311.

[29] Quadrennial Defense Review, 2006.

[30] Quadrennial Defense Review, 2006; Nathan Frier, "Hybrid Threats: Describe…Don't Define," *Small Wars Journal* (2009), 5. Of note, this author's conversations with Hybrid Theorist Frank Hoffman (Washington, DC, February 2012) included a conversation on the emergence of this quad chart concept and the idea that the original concept was more oriented toward dashed rather than solid lines separating the chart—enabling threats to move or blend from one category to another. Hybrid threats in particular are best understood if considered from this position of quantified movement.

Mr. Frank Hoffman continued the theoretical evolution of warfare through the contribution of his ideas about hybrid warfare. Hybrid warfare emerged as a military term in the 2007 U.S. Maritime strategy, describing the convergence of regular and irregular threats using simple and sophisticated technology via decentralized planning/execution.[31] Hoffman built this idea by positing hybrid warfare as the synergistic fusion of conventional and unconventional forces in conjunction with terrorism and criminal behavior.[32] This fusion is oriented toward a desired objective through a political narrative, which simultaneously and adaptively unifies all the elements of the force. Additionally, he explained that either a state or a non-state actor at the tactical, operational, or strategic level could conduct this form of warfare.[33] Hoffman's blending effect is the combination, or rather optimization, of not only regular and irregular generational forms of warfare, but also the effects of socially disruptive actions of crime and terrorism, and the resultant strategic messaging effect.[34] In essence, Hoffman's ideas of hybrid warfare build upon the construct of compound warfare to include a synergistic fusion of the elements with the inclusion of terrorism and criminal behavior. His revolutionary approach not only introduced the concept of hybrid war, but also enabled a new dialogue between the conventionally and unconventionally oriented portions of the U.S. defense establishment.[35]

In the terms of hybrid warfare, Frank Hoffman's work from 2006 until the present became the gold standard for understanding the concept of hybrid forces and the synergistic effects that they could produce. Hybrid warfare theorists writing after 2006—working in the U.S., the United Kingdom, or Israel—have used Hoffman's benchmark to orient their work in order to agree, disagree, or attempt to expand on his concepts. However, for our discussion of theory, this work is not sufficient, as it is primarily descriptive and does not capture a concise form, function, and logic to explain a hybrid organization that conducts hybrid warfare. A better explanation of hybrid organizations will come from a theory composed of principles that enable a broad understanding or rationale for hybrid organizations' existence. Much of the following professional literature on hybrid warfare builds or contrasts with Hoffman's work. British military doctrine, in contrast to Hoffman's premise, captures hybrid warfare as an aspect of irregular warfare. No true distinction is made between an irregular or guerilla force and any type of a better equipped force that uses a variation of asymmetric tactics.

> Hybrid warfare is conducted by irregular forces that have access to the more sophisticated weapons and systems normally fielded by regular forces. Hybrid warfare may morph and adapt throughout an individual campaign, as circumstances and

[31] Headquarters, Department of the Navy, *A Cooperative Strategy for 21st Century Seapower* (Washington, DC: Department of the Navy, 2007).

[32] Hoffman 2007, 301.

[33] Ibid., 301.

[34] Frank Hoffman, "Hybrid vs. Compound War," *Armed Forces Journal* (2009); Nathan Frier, "Hybrid Threats: Describe…Don't Define," *Small Wars Journal* (2009): 5; and Biddle, Stephen, and Jeffrey A. Friedman. *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy*, Carlisle Barracks, PA: Strategic Studies Institute, 2008.

[35] Often times, military forces are divided between two mindsets—those who see only the conventional threat (or at the least its primacy) and those who see only the unconventional or irregular threat. This is often a matter of institutional placement (e.g. Tank Commanders that train extensively for tank battles versus Special Forces that typically operate in insurgent type situations).

> resources allow. It is anticipated that irregular groups will continue to acquire sophisticated weapons and technologies and that intervention forces will need to confront a variety of threats that have in the past been associated primarily with the regular Armed Forces of states.[36]

As a result, the British do not consider a differing logic regarding the formation or utilization of a hybrid threat, exposing a gap in common understanding between the U.S. and its closest military ally.

Israeli military theorists describe hybrid threats and hybrid warfare as a method of social warfare which is unbounded by social constraints. Therefore, hybrid threats not only gain a physical advantage through the combination of conventional technology and organization with unconventional tactics and applications, but also gain a cognitive advantage by the very lack of social restrictions that conventional state forces must adhere to such as the Law of Land Warfare, Geneva Convention, and Rules of Engagement. Added to this dual advantage is the idea that hybrid forces operate as a networked system that is much quicker than a conventional force in utilizing and responding to popular opinion, its support base, and internal feedback or learning. This orientation toward systems thinking renders the placement of hybrid warfare on an evolutionary scale irrelevant because it only requires a cognitive basis rather than a material one normally ascribed to either a conventional or an unconventional military force. The Israeli view also points toward an effects-based understanding of the hybrid threat versus a functionally based understanding, which leads to a universal vice a tailored approach in responding to hybrid warfare. As a result, the Israeli description ultimately disagrees with U.S. points of view by focusing more on the synergy of hybrid components—to include the cognitive—in producing a military effect rather than on the differences in functional capability within the hybrid force itself.[37] This disagreement allows a useful counterpoint in the dialogue and again questions the utility and accuracy of a description, or definition, of hybrid warfare, pointing to a need for an understanding of the logic or theoretical nature of hybrid warfare rather than an overarching description that fails to transition from one case study to another.[38]

Hoffman's ideas about hybrid warfare gained traction within the U.S. defense community, and several other military theorists expounded upon these ideas. Colonel Jeffrey Cowan continues the discussion in his monograph *A Full Spectrum Air Force* in which he outlines the spectrum of conflict as envisioned by the defense analyst Shawn Brimley.[39] Brimley's model includes low-end insurgent tactics and limited technology on one end and large conventional armies with high-level technology such as nuclear weapons, bombers, and aircraft carriers on the other end. In this model, modern conventional militaries attempt to cover the middle and higher end of the spectrum to guard against

---

[36] Ministry of Defense, The United Kingdom Joint Doctrinal Note 2/07 *Countering Irregular Activity Within A Comprehensive Approach* (Shrivenham Defence Academy, Shrivenham, Wiltshire, UK, March 2007).

[37] Author's discussion with retired IDF generals and current Israeli military theorists in Tel Aviv, Israel, March 2012.

[38] *Hybrid Warfare*, Global Accountability Office, 10 September 2010. As discussed in previous footnotes, there is no universal consensus on either the existence of hybrid warfare or on its definition—this contention is global, not simply focusing on U.S. theorists, but extending through the UK, Israel, and beyond.

[39] Jeffrey L. Cowan, *A Full Spectrum Air Force* (master's thesis, Air War College, 2009) and Shawn Brimley; *Crafting Strategy in an Age of Transition* (Carlisle Barracks, PA: Parameters, U.S. Army War College Press, 2009), 28.

"most likely threats."[40] In the case of the U.S. military, the preponderance of the military forces straddle the middle portion of the model, and technological applications are used to control the higher end capabilities such as intelligence, surveillance, and reconnaissance platforms and paired high-end technology such as nuclear weapons and precision strike capabilities.

Cowan explains the model in terms of hybrid warfare by arguing that the pressures of globalization allow potential hybrid threats to gain access to conventional military capabilities that normally reside closer to the middle of the spectrum through the use of global finance and the available proliferation of information and technology. Examples include air defense systems such as the rocket propelled grenade and the Kornet Anti-tank Missile, both used by Lebanese Hezbollah in the 2006 War against Israeli Defense Forces.[41] He then explains that the globalization and the proliferation of weapons of mass destruction (WMD) technology—defined as nuclear, biological, chemical, radiological, and high explosive—have bent the high end of the spectrum toward the middle as non-state actors such as terrorists and hybrid threats compete with some Second and Third World nations to gain access to this end of the spectrum through the use of money and acquisition of available means such as technical knowledge and equipment. This idea is useful toward helping to explain the existence of hybrid warfare because of the dual pressures of globalization pressure and technological/information availability that have allowed low-end opponents to access both ends of the spectrum and to ignore the costly middle section. As a result, hybrid threats can potentially use depth to engage in conflict at almost any point on the spectrum. Cowan's assertions are useful to an initial consideration of the underlying logic of the hybrid threat and enquiry into the factors that motivate and enable the formations of hybrids.

In his monograph, *Strategic Implications of Hybrid War: A Theory of Victory*, Lieutenant Colonel Daniel Lasica posits that hybrid force actors attempt to combine internal tactical success and information effects regarding enemy mistakes through the deliberate exploitation of the cognitive and moral domains.[42] In this manner, he describes hybrid warfare simultaneously as a strategy and a tactic because of the blending of conventional, unconventional, criminal, and terrorist means and methods. A hybrid force is thus able to compress the levels of war and thereby accelerate tempo at both the strategic and tactical levels in a method faster than a more conventional actor is able to do. In this theoretical model, the hybrid actor will always gain a perceived strategic advantage over the conventional actor regardless of tactical results.[43] Again, this effort to understand the logic of a hybrid force enables a glimpse of the motivating factors which drive a hybrid threat and how it forms.

---

[40] Ibid., 28.

[41] Matthews 2008, 1-96.

[42] Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory* (master's thesis, School of Advanced Military Studies, 2009), 1-62.

[43] In the context of the 2006 War, Lebanese Hezbollah (LH) is defeated at the tactical level, arguably losing the majority of its tactical engagements with the IDF, however in a strategic sense LH is seen to have emerged from the conflict as a victor. Although this perception is adroitly put forward by LH information type operations, there is a ring of truth in the sentiment—gaining even IDF agreement as to LH's strategic victory. Discussions with U.S. and IDF military analysts confirm this finding—although in retrospect, each notes that a type of "mutual" deterrence was effected following the conflict with neither side being willing to unnecessarily return to any type of military confrontation.

David Sadowski and Jeff Becker, in their article "Beyond the "Hybrid" Threat: Asserting the Essential Unity of Warfare," expand the discussion by decrying the "quad-chart approach" which put each type of threat category in its own simple, separate "box."[44] They assert, in contrast to Brimley, that the idea of simply seeing hybrid warfare as a combination of threat categories or capabilities fails to appreciate the complexity of the hybrid approach to warfare.[45] Rather, they argue that the essential aspect of hybrid warfare is the underlying unity of cognitive and material approaches in generating effects. Such a unity of cognitive and material domains allows for flexibility in a strategic context in which social "rules" can be redefined in an iterative process to the hybrid's advantage in terms of legality and military norms.[46] The resulting flexibility facilitates iterative adaptation that allows the hybrid force to quickly take advantage of opportunities, both in terms of material equipping and in terms of cognitively influencing the environment. This combination of the cognitive and material domains in understanding is important in that it bridges the gap between U.S. and Israeli ideas and serves to expand the existing conceptions of hybrid warfare.

The 2010 QDR follows these ideas by expressing hybrid warfare as:

> the seemingly increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict. While the existence of innovative adversaries is not new, today's hybrid approaches demand that U.S. forces prepare for a range of conflicts. These may involve state adversaries that employ protracted forms of warfare, possibly using proxy forces to coerce and intimidate, or non-state actors using operational concepts and high-end capabilities traditionally associated with states.[47]

The review continues with a discussion of the multiple challenges and complex combinations of approaches and capabilities that will likely emerge from a hybrid threat. It then directs that U.S. forces must tailor themselves to react flexibly across a varied range of potential conflicts. As a formal strategic document, the QDR not only offers a mandate to explore the potentials of a hybrid threat, but in directing a response from the military force—the QDR makes understanding the logic of a hybrid threat an imperative. Defense theorists then couple the strategic QDR language with the *U.S. Army Capstone Doctrine for 2009–2025*, which attempts to translate and outline the future threats that the U.S. military will face in this period. The doctrine paints a threat picture in which "Army forces must be prepared to defeat what some have described as hybrid enemies: both hostile states and non-state enemies that combine a broad range of weapons capabilities and regular, irregular, and terrorist tactics; and continuously adapt to avoid U.S. strengths and attack what they perceive as weaknesses."[48] This functional language endeavors to create a functional definition that users can then capture within

[44] David Sadowski and Jeff Becker, "Beyond the "Hybrid" Threat: Asserting the Essential Unity of Warfare," *Small Wars Journal January 7*, 2010, 1-13.

[45] *2010 Quadrennial Defense Review*, February 2010 and Michelle Flournoy, *Contested Commons: The Future of American Power in a Multipolar World* (Washington, DC—Center for a New American Security, 2010).

[46] These social rules exist to constrain both the conceptual and the material understanding of a situation and any resulting action that takes place within a system.

[47] *2010 Quadrennial Defense Review*, February 2010, 8, 15.

[48] Headquarters, Department of the Army, *Army CAPSTONE Concept 525-3-0* (Washington, DC: Department of the Army, 2009), 15, 47.

operational and tactical doctrine that U.S. Army ground forces can employ. This offers some benefit in adding to the discourse a formal definition of hybrid threats. However, an understanding of the underlying logic is still missing—ultimately requiring a predictive theory that sets out principles that can act as a guide to explain the behavior of hybrid actors.

The military doctrine resulting from this strategic conception of hybrid organizations, *U.S. Army Field Manual 5-0: The Operations Process*, defines a hybrid threat as dynamic combinations of conventional, irregular, terrorist, and criminal capabilities adapting to counter traditional advantages.[49] *U.S. Army Field Manual 3-0: Operations* then describes hybrid threats functionally as "a diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects. Such forces combine their abilities to use and transition between regular and irregular tactics and weapons."[50] In addition,

> These forces may cooperate in the context of pursuing their own organizational objectives. Hybrid threats may use the media, technology, and their position within a state's political, military, and social infrastructures to their advantage. Hybrid threats creatively adapt, combining sophisticated weapons, command and control, cyber activities, and combined arms tactics to engage U.S. forces when conditions are favorable."[51]

As functional definitions, these documents describe a hybrid threat as a mix of military capabilities, but do not facilitate any comprehension of an underlying logic that drives a hybrid forces to manifest in a certain way. In this manner, the FM describes the symptoms of the threat, but the disease remains a mystery. As such, this monograph attempts to remedy this situation by providing a theory of hybrid warfare that will enable prediction of hybrid behavior.

A Theory of Hybrid War: New Ways of Explaining Hybrid Behavior

What follows is a proposed theory of hybrid warfare. Such a theory will provide for the elucidation of the formation and behavior of hybrid organizations. The principles which serve as the architecture of this theory will also be derived from historical trends. The resulting theory will then be explored and validated through an analysis of two case studies which represent examples of hybrid warfare. This logic will be shown through several principals derived from historical trends. The monograph then explores and validates the resulting theory through analysis of two hybrid warfare case studies. Following the review of available military theories on the different forms of warfare, it is appropriate to return to one of the most respected military theorists on war to construct a theory of hybrid warfare. Clausewitz defined war as "an act of force to compel

[49] Headquarters, Department of the Army, *The Operations Process 5-0* (Washington, DC: Department of the Army, 2008), 3, 4.

[50] Headquarters, Department of the Army, *Operations 3-0* (Washington, DC: Department of the Army, 2011), 1-5.

[51] Ibid. 1-23 For example, criminal elements may steal parts for a profit while at the same time compromising the readiness of an adversary's combat systems. Militia forces may defend their town with exceptional vigor as a part of a complex defensive network. Additionally, hybrid threats use global networks to influence perceptions of the conflict and shape global opinion.

our enemy to do our will."[52] He theorized that the ultimate expression of war is "ideal" or "absolute" war where all available resources and assets are applied to achieve the desired end state of the war. However, Clausewitz stated that this ultimate expression of war would often be counter to the desired political ends of a war thereby making it unrealistic, so he outlined the concept of "limited war" in which militaries optimize available means to meet limited political goals. As a result, the generalized categories of "ideal" or total war, "limited war," and military operations that occur underneath a level of declared war have come to be accepted generalizations regarding warfare. This idea of "limited war" with its inherent ideas of social constraint and thresholds of military potential has the most contemporary significance in the construction and employment of military organizations.[53]

In war, a state actor will generally match available means—defined by a portion of gross domestic product matched to technological capability—to projected political end-states—contingency requirements planned against potential adversaries in a multitude of contexts. As a result, the typical military organization will be optimized for a broad range of potential scenarios based on likely political temperament. In a large, resource rich country such as the U.S., China, or Russia, this results in a broad force which is prepared for offense, defense, and stability type operations across a varying scale. In reality, this "optimized" force is not prepared for a specific employment context, but rather optimizes to best meet a broad array of scenarios for employment—resulting in less optimization for a unique context.

However, not all military organizations develop or are employed in this manner. Nations constrained by a lack of resources or technological capability must make decisions as to the breadth and depth of their "optimization." This practice can then lead to a number of variations in military organization from broad, flat armies of primarily light infantry designed for specific functions such as population control and internal regime survival, to small or medium sized forces with combined arms depth to confront specific external threats such as tanks, missiles, and aircraft. Generally, these less resourced organizations will conform to a conventional model of a large, full-spectrum military on a smaller scale as in the example of the 1973 era Egyptian Army based on a Soviet-type organizational model.[54]

In some cases, organizations will develop optimized military structures outside conventional models. These unconventional structures will be optimized to a specific,

[52] Carl von Clausewitz, *On War,* trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 24–25, 65–67.

[53] Specifically, the idea of limited war refers to the historical observation that war as a social construct is self-regulating to a certain degree. It requires the acquiescence of its participants and supporters to escalate from one level to another and as such will meet certain thresholds of either military capability or resource availability. These thresholds will in effect limit the scope of the war. Most state actors or non-state actors will recognize some of these thresholds and attempt to optimize their behavior and organizations within these constraints (laws, budgets, popular support, international opinions, et cetera).

[54] George W. Gawrych, *The 1973 Arab-Israeli War: The Albatross of Decisive Victory* (Fort Leavenworth, KS: Combat Studies Institute Press, 1996). In the buildup to the 1973 Arab-Israeli War, Egypt was able to look at Israel previous air and land power success and was able to optimize the Egyptian Army and its war plan for the 1973 war. In doing so, the Egyptians maximized their anti-tank and anti-air capabilities using Soviet supplied arms and then operationalized that capability in limited advances under the protection of these weapon systems. The result was shocking to the military world in that the relatively advanced Israeli Defense Force was beaten by the sub-par Egyptian Army that the Israelis had resoundingly beaten in 1967.

contextual purpose but utilize resources and capabilities that are not contained in a conventional military force. Observers often refer to these unconventional organizations as asymmetric or hybrid threats that offer certain advantages to automatically alter the battlefield calculus when confronting a more conventional force. These observers then often refer to the resulting conflict as hybrid war. In other words, a hybrid war can best be described as an optimized form of warfare that allows a combatant to attempt to utilize all available resources—both conventional and unconventional—in a unique cultural context to produce specific effects against a conventional opponent.

In order to begin to understand hybrid warfare, it is necessary to engage in a deeper enquiry into the reasons a hybrid force forms, or is formed. Logic would seem to indicate that a hybrid force is formed to generate specific effects upon a battlefield or directly on an enemy combatant. The formation of this force would be constrained by both the available means at its disposal and envisioned in ways that those means could be applied to achieve desired ends.[55] For the hybrid force, this process of formation is different from conventional and irregular warfare in that the constraints and motivations that drive the hybrid force do so with a unique logic—as explained in the theories' principles.

Historically, the hybrid formation process has resulted in several commonalities in terms of composition and effects, which in turn can be generalized into seven principles to describe hybrid war in its totality.

The first principle of hybrid war proposed here is that a hybrid force's composition, capabilities, and effects are unique to the force's own specific context. This context relates to the temporal, geographic, socio-cultural, and historical setting in which the given conflict takes place.

The second principle is that there exists a specific ideology within the hybrid force that creates an internal narrative to the organization. This ideology is inherently linked to the strategic context and is grounded within the socio-cultural, religious identity of the hybrid force. The resulting narrative serves to redefine the extant rules within the strategic context.

The third principle is that a hybrid force perceives an existential threat by a potential adversary. This perceived threat drives the hybrid force to abandon conventional military wisdom to achieve long-term survival.

The fourth principle is that a capability overmatch between the hybrid force and a potential adversary exists. The hybrid force contains less conventional military capability in comparison to its adversary and therefore must seek a way to offset this apparent advantage in military capability.

The fifth principle is that a hybrid force contains both conventional and unconventional elements. These elements often comprise "accepted" military technology and nonmilitary, guerrilla type technology. The elements may also include the use of terrorist or other criminal tactics. These combined capabilities create an asymmetric advantage for the hybrid force.

[55] The desired ends of a hybrid organization are often political in nature—relating to the popular motivations both within the organization itself and in the populace that exists around the hybrid organization.

The sixth principle proposes that hybrid organizations rely on inherently defensive type operations. The hybrid force seeks to defend its existence and employs an overall strategy of defensive operations. These operations will often include offensive components, but the overarching intent is still one of defense.

The seventh principle is that hybrid organizations use attritional tactics in the employment of the hybrid force. These tactics manifest in both the physical and the cognitive domains in order to continually whittle away the adversary's forces and his will to use them.

Therefore, hybrid war theory may be best summarized as a form of warfare in which one of the combatants bases its optimized force structure on the combination of all available resources—both conventional and unconventional—in a unique cultural context to produce specific, synergistic effects against a conventionally-based opponent.

Analysis Methodology

What follows is a historical analysis of selected case studies that is both qualitative and deductive. This analysis will provide additional insights that will contribute to the development and refinement of the theory of hybrid warfare proposed in this work. The case studies explored are Lebanese Hezbollah in the 2006 Israel-Hezbollah War and the Soviet partisan network during World War II on the Eastern Front from 1941 to 1945. The Lebanese Hezbollah case study is the original instance of hybrid warfare and as such has served as ground zero for much of the work on hybrid warfare and hybrid organizations. The Soviet partisan network case study is a historical example of hybrid warfare that has not been analyzed in detail—this review will serve to offer an untouched example of hybrid warfare to be explored by the proposed theory to determine the universal applicability of its principles. This process offers supporting evidence via concrete example of each of the proposed principles that support the theory. As a result, the theory of hybrid warfare will be not only validated, but will also be shown to be broadly applicable in historical analysis.

2. The Israel-Hezbollah War (2006): A Well-Trod Example Revisited

Following the review of literature on evolving modern warfare and the existence of hybrid warfare as a component of modern conflicts, this monograph now conducts a qualitative and deductive analysis of historical case studies to explore and validate the proposed theory of hybrid warfare. In doing so, it attempts to parse examples of each principle to show its existence within the historical context of the case study. The monograph first examines Lebanese Hezbollah as the prototypical hybrid organization during its conflict with Israel in the summer of 2006. As the analysis will show, Lebanese Hezbollah functions as a hybrid organization and as a result manifests multiple synergistic advantages in relation to its opponent. In teasing out the motivations for these functional behaviors, Lebanese Hezbollah validates the proposed theory by demonstrating the qualitative presence of each of the principles. The summary at the end of this chapter provides a holistic synthesis by showing the relevance of the hybrid actor within the historical context.

Strategic Context of the Israel-Hezbollah War

To understand the depth of this conflict, we will first review the strategic context of the situation so that understanding may be gained when looking for the presence of the proposed theory and principles. The Israel-Hezbollah War of 2006 was a 34-day military conflict, which pitted the pre-eminent conventional military force in the Middle East—Israel—against the combined conventional and unconventional military force of the non-state actor Lebanese Hezbollah. The conflict began when Lebanese Hezbollah conducted attacks against Israeli border forces and kidnapped two Israeli soldiers on 12 July 2006. Israel responded with a failed rescue attempt and a synchronized air and ground bombardment of Southern Lebanon, followed by a ground invasion and a naval blockade of Lebanon. Lebanese Hezbollah retaliated with massive rocket strikes into Northern Israel and a guerilla campaign utilizing prepared, hardened defensive positions. Fighting continued until regional and international pressure resulted in a United Nations brokered ceasefire on 14 August 2006.[56]

In total, the fighting resulted in the deaths of approximately 1,200 people. The fighting displaced over a million people in Southern Lebanon and in Northern Israel. On the Israeli side, 114 Israeli Defense Force soldiers were killed and significant amounts of Israeli military equipment were damaged or destroyed, including up to 10 percent of Israel's committed main battle tanks, and some rotary wing aircraft and coastal naval vessels were severely damaged.[57] More than 40 Israeli civilians were killed and nearly 4,000 were injured in addition to an estimated $3.5 billion loss in war cost and economic output.[58] In Lebanon, Lebanese Hezbollah suffered contentious losses of between 46 and 600 fighters killed, and its observed military capability was estimated to have been reduced by one half.[59] In addition, over 1,000 Lebanese civilians were reportedly killed and over 4,000 were injured in addition to an estimated $4 billion loss in buildings and infrastructure.[60]

The conflict played out against a historical backdrop of political, religious, and ethnic tensions between the strong state actor, Israel, and the ambiguous non-state actor, Lebanese-Hezbollah within the neighboring weak state of Lebanon. Israel is a strong, Jewish state in a contested geographic area, which has historically fought for survival against the Arab and Muslim populations of the Middle East. Israel generally comprises a dominant Jewish demographic and is supported by both a strong internal economy and by external remittances and patronage.[61] Israel's military industrial complex is the most advanced within the Middle East region, fielding advanced ground, air, and sea platforms, making it a powerful conventional military force capable of both internal and external defense on multiple fronts.

---

[56] Matthews 2008, 1-96.

[57] Ibid., 20.

[58] Harel Amos and Avi Issacharoff, *34 Days: Israel, Hezbollah, and the War in Lebanon*. (New York: Palgrave Macmillan, 2008.), 1-304.

[59] Ibid., 1-304; Matthews 2008, 29.

[60] Uri Bar-Joseph, "The Hubris of Initial Victory: The IDF and the Second Lebanon War," in *Israel and Hizbollah*, ed. Clive Jones and Sergio Catignani, (London: Routledge, 2010), 156-159.

[61] Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/is.html on 5 April 2012. The CIA World Factbook list Israel's population demographics as 76 precent Jewish, 20 percent Arab—although almost all policy is Jewish.

Lebanon is a weak, multicultural state, which has been a confluence of both Mediterranean and Middle Eastern peoples and beliefs for centuries. This cultural milieu has resulted in a demographic mix that tentatively balances between multiple Muslim and Christian factions within the population.[62] As a result, Lebanon has a relatively weak central government and with control distributed among many factions according to the 1926 Lebanon Constitution. During the civil war of 1975–1990, this balance of power was contested. Following the 1979 Iranian Islamic Revolution, additional pressure was placed on the balance of power via the Shi'a demographic. This in turn has led to external interference and sometimes domination of Lebanon by her stronger neighbors, Syria and Israel—perpetuating the cycle of a lack of control and resulting in historically poor infrastructure. The weak governmental structure is mirrored by a relatively weak military that lacks not only the power to conduct external defense, but also to impose or support internal order—effectively creating an internal power vacuum. Lebanese Hezbollah filled the power vacuum created by this lack of internal political and military strength in the early 1980s.[63]

Lebanese Hezbollah is a strong militia with political aspirations, founded in 1982 in response to Israeli actions in Lebanon. The group quickly emerged as both a legitimate political entity and as a credible military force.[64] Although not possessed of internal means of generating large-scale military power, Lebanese Hezbollah has continuously received equipment, training, and funding from its anti-Israeli allies—Iran and Syria. As the group's military prowess matured over time, it gained significant conventional capabilities in terms of rockets, artillery, anti-aircraft, anti-ship, and anti-tank weaponry. This conventional capability is augmented by an asymmetric capability including criminal/terrorist activities and networks.[65] As a result, the unique picture of Lebanese Hezbollah is built to show its attributes as a hybrid organization.

Hybrid Principles in Detail

When analyzed as a hybrid force, Lebanese Hezbollah displays several strong characteristics within the context of the Israel-Hezbollah 2006 War.

The first principle of hybrid war is that a hybrid force's composition, capabilities, and effects are unique to the force's own specific context. This context includes the temporal, geographic, socio-cultural, and historical setting in which the given conflict take place. Lebanese Hezbollah exists within just such a specific enabling context. The weak central government and conflicted lines of power within the country allow Lebanese Hezbollah to exist peaceably and to easily maintain and improve its militant status and freedom of action. Lebanon itself is not only a cultural and demographic mix of Eastern

[62] Retrieved from https://www.cia.gov/library/publications/the-world-factbook/geos/le.html on 5 April 2012. In large part due to the nature of its weak central government, the preservation of the 1932 census and its resulting balance of power is preferred by most of Lebanon's population. For this reason, any changes in population demographics (primarily from Christian to Muslim majorities) are masked to maintain the historical partitioning of government positions between the population demographics. As a consequence, the central government remains weak and highly partisan.

[63] Ahmed Nizar Hamzeh, *In The Path of Hizbullah*. (Syracuse, NY: The Syracuse University Press, 2004), 43.

[64] Penny L. Mellies,"*Hamas and Hezbollah: A Comparison of Tactics*." *In Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, edited by Scott C. Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, 2009), 1-146.

[65] Matthews 2008, 1-96.

and Western society, but it also rests within the arc of a large Shi'a Muslim demographic density that extends from Lebanon through Syria, Iraq, Iran, and Bahrain—otherwise known as the "Shi'a Crescent."[66] The "Shi'a Crescent" serves to unify Lebanon's internal Shi'a Muslim population allowing Lebanese Hezbollah a solid base of support—and then extends this support base through to its external sponsors, Syria and Iran. In addition, the ideology espoused by Lebanese Hezbollah extends to the Lebanese diaspora throughout the world and engenders both sympathy and support for the organization.[67]

The second principle of hybrid posits that a specific ideology exists within the hybrid force that creates an internal narrative to the organization. This ideology inherently links to the strategic context and is grounded within the socio-cultural, religious identity of the hybrid force. The resulting narrative redefines the extant rules within the strategic context. Lebanese Hezbollah maintains an ideology of righteous Islamic Revolution grounded in both its assumed role as an anti-Israeli militia and as a Shi'a protector in Lebanon.[68] This narrative supports both the external and internal support relationships as well as facilitating the growth and control requirements of Lebanese Hezbollah as a dominant non-state actor within Lebanon.

The third principle of hybrid warfare is the hybrid force's perception of an existential threat by a potential adversary. This perceived threat drives the hybrid force to abandon conventional military wisdom in order to find ways to achieve long-term survival. In the case of Lebanese Hezbollah, Israel established a long historical precedent of military action and occupation in Lebanon in 1948 during the Arab-Israeli War with the Israeli occupation of numerous southern border villages in Lebanon.[69] The invasion of southern Lebanon followed in 1978 and occupation of territory south of the Litani River.[70] In 1982, a large Israeli ground force briefly entered the eastern portion of Beirut, the capital of Lebanon.[71] The Lebanese people and Lebanese Hezbollah can see Israel as an existential threat if it combines selected historical facts with Israeli policy statements. Moreover, Lebanese Hezbollah could go so far as to identify an Israeli threat to the Lebanese population writ large. In fact, Lebanese Hezbollah's vibrant public rhetoric regularly incorporates this understanding.[72] The realization of this existential threat thereby prompts Lebanese Hezbollah to seek any method possible to defend itself—including both conventional and unconventional methods. Another result of this rhetoric and understanding is the tacit approval of the approval of the Lebanese people—which creates a support base that enables the actions of Lebanese Hezbollah, including the unconventional, terrorist, and criminal activities that support the organization.

[66] Ibid., 15-18.

[67] Amos and Issacharoff 2008, 76-121.

[68] Mellies, 2009.

[69] Daniel Isaac Helmer, *Flipside of the COIN: Israel's Lebanese Incursion Between 1982–2000.* (Fort Leavenworth, KS: Combat Studies Institute Press, 2007), 1-85.

[70] Ibid., 64.

[71] Amos and Issacharoff 2008, 76-121.

[72] Retrieved from http://www.state.gov/r/pa/ei/bgn/35833.htm on 5 April 2012. Outlines ISR policy statements—many of which espouse the destruction of Hezbollah and any other threat to Israeli security. These policies are available to the public domain and are often published in both Israeli and Lebanese periodicals.

Principle four posits that in a hybrid war there exists a capability overmatch between the hybrid force and a potential adversary. The hybrid force contains less conventional military capability compared to its adversary and therefore must seek a way to offset this apparent advantage in military capability. In the case of Lebanese Hezbollah and Israel, this overmatch is readily apparent. Israel not only maintains a large internal military industrial complex, but also links through close alliances to both the American and European military industrial complexes—thereby being capable of maintaining a relatively large conventional army.[73] Lebanese Hezbollah on the other hand, maintains an ad-hoc militia force that is reliant on external arms supplies and unconventional techniques to achieve military effects.[74]

The fifth principle says that a hybrid force contains both conventional and unconventional elements. These elements often comprise "accepted" military technology and nonmilitary, guerrilla type technology and tactical application. These combined capabilities create an asymmetric advantage for the hybrid force. In a ground force comparison of the 2006 War, Israel fields an army containing main battle tanks such as the Sabra Mark I and Merkava Mark IV, armored personnel carriers like the Namer, infantry fighting vehicles such as the Golan Armored Vehicle, towed and self-propelled artillery systems like the LAROM and Sholef, and multiple variations of unmanned aerial drones.[75] Additionally, Israel maintains multiple air force strike fighters such as the Kfir and F-16I, rotary wing platforms, and coastal defense ships.[76] Conversely, Lebanese Hezbollah utilizes multiple small arms variants, anti-tank munitions, anti-aircraft systems, anti-ship weapon systems, and multiple rocket and missile platforms.[77] These elements combine in a mixed hierarchical/cellular structure comprised of both conventional fighters and irregular militia. The more conventional fighters are capable of advanced application of their weapon systems, as seen in the example of 3709 rocket attacks launched into Northern Israel—hitting 901 towns and cities during the 34-day conflict.[78] The irregular militia units use improvised explosive devices (IEDs) and are capable of near simultaneous swarming attacks.[79]

Hybrid forces seek to use defensive type operations; this is the sixth principle of hybrid warfare proposed in this work. The hybrid force seeks to defend its existence and will employ an overall strategy of defensive operations. These operations will often include offensive components, but the overarching intent will still be one of defense. In the 2006 Israel-Lebanese Hezbollah War, Lebanese Hezbollah fought from prepared fighting positions, including fortified bunkers, which were arranged in depth in Southern Lebanon.[80] From these defensive positions, Lebanese Hezbollah launched multiple rocket attacks and executed swarming attacks against Israeli ground forces. As such, these operations primarily focused on the overall survival of Lebanese Hezbollah forces or on the protection of their corresponding local support networks. It is noteworthy

[73] Matthews 2008, 12, 47-56.

[74] Amos and Issacharoff 2008, 47.

[75] Mellies 2009, 1-146.

[76] Ibid., 97.

[77] Amos and Issacharoff 2008, 76-121.

[78] Matthews 2008, 1-96.

[79] Helmer 2007, 1-85.

[80] Ibid., 47.

that, although Lebanese Hezbollah attempted to defend several village locations, it did not necessarily defend them to the death, but rather would often attempt to break contact to avoid being killed by Israeli Defense Forces—in order to be able to fight in a future engagement.[81] Generally, all ground engagements occurred when Israeli Defense Forces entered into areas occupied by Lebanese Hezbollah fighters.[82] Rocket attacks were offensive in nature, but were launched for the stated purpose of retaliatory strikes against Israeli forces in Lebanon in the context of contested areas such as Shaba Farms or the Golan Heights and as such can be viewed as overall defensive operations.

Lebanese Hezbollah relied on attritional tactics throughout the Israel-Lebanon 2006 War, and this too is consonant with the proposed hybrid warfare theory. Principle seven emphasizes the use of attritional tactics in the employment of the hybrid force. These tactics manifest in both the physical and the cognitive domains to continually whittle away the adversary's forces and his will to use them. In the case of Lebanese Hezbollah, the physical manifestation of these attritional tactics occurred using mine and improvised mine warfare, mass use of indirect fire attacks—missiles, rockets, and mortar fire, and the use of anti-tank/anti-personnel ground ambushes.[83] None of these techniques were planned or executed to be decisive ground actions, but rather were engaged in as opportunity attritional targets. As such, Lebanese Hezbollah rarely massed outside of occasional swarming attacks which were multi-directional—as in the attacks along the southern Lebanon border.[84] Added to this were the cognitive aspects of attritional tactics in the use of the initial kidnapping of two Israeli Defense Force soldiers, the historical threat of the use of suicide bombing, the repeated bombardment of Israeli civilian populations, and the rapid use of media to execute strategic information influencing operations.[85] In this case, attritional tactics also served to exploit gaps in conventional force Israeli logic and thereby served to extend the conflict to the benefit of Lebanese Hezbollah.

How Effective Were They? The Effects of Hybrid Principles

Synthesizing the seven principles of hybrid warfare within the context of the 2006 Israel Lebanese Hezbollah War, the David and Goliath image of a weaker opponent besting a stronger one becomes quite clear. Although Lebanese Hezbollah received more damage than the Israel Defense Forces and was tactically defeated on multiple occasions throughout the 34-day conflict, Lebanese Hezbollah was able to take advantage of several critical factors in order to gain an operational and strategic victory. Despite their clear military and economic advantages, the Israeli Defense Forces were unable to meet the operational and strategic objectives of the military defeat of Lebanese Hezbollah. The court of public opinion in Israel, Lebanon, and throughout the world saw Israel as losing the conflict.[86] As a hybrid force, Lebanese Hezbollah was able to use its internal

[81] Matthews 2008, 33-39.

[82] Ibid., 33-39.

[83] Mellies 2009, 98-121.

[84] Ibid., 87.

[85] Helmer 2007, 1-85.

[86] Mellies 2009, 83-99.

strengths of narrative, weapons mix, and tactics to overcome the weaknesses of its much stronger opponent.

Through asking why or how this happened, it becomes clear that Lebanese Hezbollah optimized its military organization to fight against a Western style conventional military organization. It did this through a combination of available equipment like anti-tank, anti-aircraft, anti-ship, and unconventional weapons—IEDs—and flexible defensive tactics like fortified defense in depth and ambush type tactics. This was coupled with an adaptive use of media exploitation and messaging in combination with a near continuous rocket bombardment.[87] The umbrella of Lebanese Hezbollah's strategic objective contained these actions to prove that it could fight against Israel and survive. In doing so, Lebanese Hezbollah was able to bind the strategic objective of victory within the internal narrative of a Shi'a protector fighting against the existential threat of Israel. As a result, Lebanese Hezbollah acted as an agile, adaptive, and lethal opponent that only had to continue to fight in order to achieve its objective and defeat its enemy. In this sense, the hybrid force gained a clear advantage through synergistic effects over its conventional opponent and achieved "victory" within the war.

3. World War II Eastern Front (1941–1945): A First Look at the Soviet Partisan Network as a Hybrid Organization

This monograph now conducts a qualitative and deductive analysis of historical case studies to explore and validate the proposed theory of hybrid warfare. In doing so, it attempts to parse examples of each principle to show its existence within the historical context of the case study. This case study examines the Soviet Partisan movement as a hybrid organization during World War II. It was selected because of its potential as a hybrid force that has not been previously analyzed. As a result, it offers a pristine example to which the proposed theory of hybrid warfare can be applied. The consequent analysis both confirms the Soviet Partisan movement as a hybrid force and validates the proposed theory and its attendant principles as being qualitatively present. A holistic synthesis also shows the relevance of the hybrid actor within the historical context—emphasizing the synergistic advantages that hybrid actors obtain versus a conventional force.

Strategic Context of the Soviet Partisan Movement

The Soviet Partisan movement during World War II was a component of the Soviet war effort against Nazi Germany from 1941–1945.[88] In this conflict within World War II, the massive conventional forces of Nazi Germany fought against the massive conventional forces of the Soviet Union, which was augmented by the Soviet Partisan movement.[89] The war on the Eastern Front in 1941 began with the German invasion of the Soviet-controlled Baltic states of Estonia, Latvia, Romania, and Lithuania, as well as former Polish territory.[90] German armies attacked deep into the Soviet Union, decimating the

[87] Ibid., 83.

[88] Earl F. Zeimke, *Stalingrad to Berlin: The German Defeat in the East,* (Washington, DC: U.S. Army Center of Military History, 2002), 3-22.

[89] Edgar M. Howell, *The Soviet Partisan Movement: 1941–1945,* (Bennington, VT: Merriam Press, 1999), 6-11.

[90] Zeimke 2002, 23.

population and threatening the survival of the Slavic nations and peoples. The Soviet Union responded with conventional military operations and irregular partisan operations.[91] The combined effect of these actions enabled the Soviet Red Army to counter-attack and regain control of lost territories. The conflict culminated in 1945 with the destruction of the Germany Army and occupation of Germany. In total, the war on the Eastern Front was the largest conventional military conflict in history and it resulted in an estimated 30 million deaths and the destruction of billions of dollars of infrastructure.[92]

In context, the German Army of the late 1930s and 1940s was the premier conventional military organization in the world.[93] As compared to the Red Army's contemporary turmoil, Germany's army had a centuries-old military tradition extending back to the Kingdom of Prussia and Frederick the Great. Innovative technology augmented this extensive martial tradition in the form of Panzer, Panther, and Tiger tanks; towed and self-propelled artillery; fighter and bomber aircraft; and multiple individual and crew-served weapons systems.[94] In terms of concurrent experience, the German Army successfully invaded Poland in 1939 and had successfully dominated France in May of 1940, arguably controlling all of continental Europe by the end of 1940—denoting not only structural proficiency, but also successful experience in the near term. This dominant military structure was governed by the ideology of the Nazi Party, which espoused world domination by the German "master race" of the Third Reich in order to restore German prestige following its defeat in World War I.[95] Generically, the Nazi ideology can be considered a fascist movement which combined nationalism and anti-communism with multiple flavors of professed racism and anti-Semitism. The resultant belief structure within the military united conventional action and presented a single narrative to its adversary, the Red Army.

The Soviet Red Army of the early 1940s presents a much different picture. The near term history of the Red Army was framed by the Russian revolution of 1917, five years of civil war ending in 1923, and then 15 years of mass industrialization and sociopolitical suppression.[96] During the 15 years of Stalin's sociopolitical engineering of the communist system, nearly 11 million people were killed or imprisoned, including vast swathes of the Red Army. The dominant ideology was that of the Communist Party as interpreted by Joseph Stalin. Generically interpreted, communism—Leninism/Marxism—can be described as an ideology that advocated a classless, stateless, atheist social order with common ownership of all state resources. In practice, this ideology in combination with Stalin's fear of a military or political coup resulted in several lethal purges within the Soviet military of anyone who voiced any type of disagreement.[97] As a result, the Red Army as an institution was devastated by the end of 1940 and was lacking in internal military strategic leadership. Additionally, the armored tank based force was primarily

[91] Ibid., 3-22.

[92] David Glantz and Jonathan House, *When Titans Clashed: How The Red Army Stopped Hitler,* (Lawrence, KS: University of Kansas Press, 1995), 5-48.

[93] Ibid., 5-48.

[94] Ibid., 41.

[95] Ibid., 47.

[96] Howell 1999, 4-22.

[97] Glantz and House 1995, 49.

made up of the T-26 and BT tanks which were technologically inferior to contemporary German tanks—although the T-34 tank was in limited use at the time and was roughly equivalent to later Panzer tank models.[98]

The Soviet Partisan element emerged in 1941 in areas behind the German front as it pushed into Soviet territory. What became known as the Soviet Partisan network was composed of several elements including bypassed Red Army troops and political commissars, small groups of airborne units dropped behind German lines, and frustrated local workers and volunteers led by members of the People's Commissariat for Internal Affairs, Stalin's Secret Police enforcers.[99] These disparate elements were brought together by their political ideology and the common threat of elimination by the occupying German forces. As the Partisan network formed, it initially operated as a semi-autonomous element conducting multiple harassing and attritional type activities against the occupying German Army.[100] As control began to be asserted through the local Communist political apparatus, these conventional and guerilla units formed into "annihilation" battalions that aimed to both destroy any resources which were available to the German Army and to disrupt German Army communications and command and control. To this end, the Partisan network used available conventional weaponry that had been left behind by retreating Red Army units, within a conventional Red Army organizational structure, and paired these with guerilla style tactics such as raids and ambushes. Many portions of the network, when unable to gain voluntary local support, turned to the use of criminal and terror type activities in order to supply themselves and coerce local support for their militant activities.[101] In doing so, the Soviet Partisan network formed itself into a hybrid force by 1943 that achieved significant disruptive effects against the German Army. These effects would later be synchronized with Red Army combat operations to create a synergistic effect in driving the German Army out of Soviet territory.[102] As a result, the Soviet Partisan network is validated as a successful hybrid organization that demonstrates the qualitative presence of the proposed principles of hybrid warfare.

The Currency of Soviet Partisan Success: Show Me the Rubles

When analyzed as a hybrid force, the Soviet Partisan network displays several strong characteristics within the context of the Eastern Front during World War II.

The first principle of hybrid war is that a hybrid force's composition, capabilities, and effects are unique to the force's own specific context. This context includes the temporal, geographic, socio-cultural, and historical setting in which the given conflict take place. The Soviet Partisan network formed in just such a specific enabling context. The historically harsh terrain of the eastern Russian steppes formed a unique context in which alternately both conventional and unconventional operations could successfully occur varying between the broad plains and the broken swathes of river and forest tracts.[103] In

[98] Howell 1999, 23-31.

[99] Ibid., 23-31.

[100] Zeimke 2002, 23.

[101] Howell 1999, 4-134.

[102] Ibid., 5.

[103] Ibid., 8.

this manner, it was inevitable that large conventional formations operating in the open terrain would eventually be paired with complementary irregular forces operating in the pockets of dense broken terrain, which existed in the steppes. The Russian experience in World War I, 1914–1917, the 1917 civil war within the Russia, and the spread of communism under Joseph Stalin had the effect of militarizing the Soviet population and instilling a level of instinctive discipline. This unique circumstance enabled the recruitment of much broader portions of the available population to form the hybrid Partisan network than would have otherwise been available.[104]

The second principle posits that a specific ideology exists within the hybrid force that creates an internal narrative to the organization. This ideology is inherently linked to the strategic context and is grounded within the socio-cultural, religious identity of the hybrid force. The resulting narrative serves to redefine the extant rules within the strategic context. In examining this principle, we return to the ideology of Communism as applied by Joseph Stalin. Communism itself merged the ideas of government and the ownership of resources, enabling a broad range of components such as people and physical resources, which could be used to form a hybrid force. Under Stalin, this ideology was magnified to an extreme which manifested itself through government enforcement via mass brutality at both the individual and collective level.[105] As a result, a narrative was crafted in which the overt loyalty of any Soviet citizen was absolute pending the threat of dire consequences. In a sense, the overt display of loyalty to the communist party as a result of nationwide paranoia became a religion in and of itself—even though the ideology itself was atheist. In combination, the ideology and the paired narrative made both loyal personnel and physical resources readily available to any entity which supported the state's desires—specifically to both the Red Army and the Partisan Network.

The third principle is the hybrid force's perception of an existential threat by a potential adversary. This perceived threat drives the hybrid force to abandon conventional military wisdom in order to find ways to achieve long-term survival. In this example, the Partisan network was clearly motivated by the existential threat posed to them by the German Army and the Nazi government.[106] Conceptually, the Soviet leadership and the citizenry could perceive this threat through the published work of the Nazi leader, Adolf Hitler. In *Mein Kampf* and *Zweites Buch*, Hitler identified Jewish people including Slavic Jews as a target for elimination. In a much more specific sense Hitler outlined the concept of *Lebensraum* which called for the creation of a German "living space" in the Soviet Union and the required elimination of the "flawed" Slavic regime that controlled the region. Following the breaking of the German-Soviet Non-aggression Pact and the invasion of Soviet-controlled Poland, practical examples of this professed philosophy played out.[107] Individual Slavic Jews were taken to concentration camps, the existing Communist governments in the conquered territories were destroyed, and party members were eliminated. In a further practical example of the existential threat posed upon the Soviet populace, the "Hunger Plan" as outlined in Operation Barbarossa was put into effect during the invasion in 1941—prioritizing all food production and consumption

[104] Ibid., 5.

[105] Glantz and House 1995, 1-14.

[106] Ibid., 28-48.

[107] Howell 1999, 43-63.

for the German Army and the German homeland over local citizens—effectively starving the local population.[108] These conceptual and practical examples clearly motivated the hybrid Soviet Partisan organizations as they realized that few viable choices were available to them in surviving life under German occupation in the Eastern Front.

Principle four posits that in a hybrid war that there exists a capability overmatch between the hybrid force and a potential adversary. The hybrid force contains less conventional military capability in comparison to its adversary and therefore must seek a way to offset this apparent advantage in military capability. With the defeat and retreat of the Red Army in 1941 and 1942, the only remaining Soviet military force was the hybrid Soviet Partisan network. The Partisan network had access to some battlefield remnants, available small arms, limited numbers of horses, and limited local supplies.[109] In contrast, the German Army was possessed of a massive conventional armory of tanks and airplanes, and benefitted from both the conventional military supply system and the locally imposed government systems which exerted control over local resources.[110] As a result, a clear overmatch in capability existed at both the offensive and logistical level between the semi-isolated Soviet Partisan network and the relatively unimpeded German Army.

The fifth principle states that a hybrid force contains both conventional and unconventional elements. These elements are often composed of "accepted" military technology and nonmilitary, guerrilla type technology. The elements may also include the use of terrorist or other criminal tactics. These combined capabilities create an asymmetric advantage for the hybrid force. In the case of the Soviet Partisan network, this principle is fairly clear-cut. The hybrid force comprised elements of bypassed Red Army units and Airborne units which were organized and equipped as conventional military units.[111] The Soviet Partisans were also composed of volunteers and political party members who had no military training and were equipped with whatever weapons became available, including old World War I weapons and recently captured German small arms. Both elements utilized a mixture of conventional military tactics such as raids and ambushes, along with irregular activities such as sabotage and harassing attacks.[112] The network also commonly stole food and local resources, as well as conducting terror and intimidation type activities against known German sympathizers.

Hybrid forces seek to use defensive type operations; this is the sixth principle of hybrid warfare proposed in this work. The hybrid force seeks to defend its existence and will employ an overall strategy of defensive operations. These operations will often include offensive components, but the overarching intent will still be one of defense. In the case of the Soviet Partisan network, this principle can be recognized in the fact that the majority of the small scale operations executed by this hybrid organization were conducted with the primary intent of ensuring the survival of the organization. The secondary purpose was in buying time for the return of the Red Army—in essence defending any currently held resources and small territories until a larger liberation

[108] Ibid., 43-63.

[109] Zeimke 2002, 103.

[110] Howell 1999, 43-74.

[111] Glantz and House 1995, 65.

[112] Howell 1999, 88-128.

could be effected through the return of the Red Army.[113] As a result, the operationally defensive orientation of this hybrid organization is revealed in the intent of its sometimes offensive operations.

The Soviet Partisan movement relied on attritional tactics through the duration of that conflict on the Eastern Front. This is consistent with the seventh principle of hybrid warfare in that hybrid organizations utilize attritional tactics to gain advantages in the employment of the hybrid force. These tactics will manifest in both the physical and the cognitive domains in order to continually whittle away the adversary's forces and his will to use them. The overarching Soviet intent for the organization was to degrade German command and control and to disrupt the German Army's rear area. In the example of the Soviet Partisan network, the attritional nature of this hybrid organization manifests itself in the repeated attacks on German Army supply lines and rear echelon formations.[114] These attacks were mostly conducted as small-scale raids and ambushes against German forces. Ultimately, this attritional strategy helped to enable Red Army victories during Operation Bagration and subsequent offensive operations by both distracting the German Army and keeping it occupied in protecting its flanks and rear areas.

The Synergistic Effects of Hybrid Principles in Action

Synthesizing the seven principles of hybrid warfare within the context of the Eastern Front of World War II, the true strength and applicability of hybrid organizations becomes clear. In this case study, the hybrid Soviet Partisan network was able to disrupt the German Army, the pre-eminent conventional military force of World War II, and enable the ultimate victory of the Soviet Red Army by shaping the German rear area from 1941–1944. Although the Soviet Partisan network did not achieve any type of unilateral victory over the German Army, it did achieve limited tactical success and enabled both the operational and strategic military success of the Red Army.[115] In essence, the Soviet Partisan network stole German momentum and created operational space for the Red Army to build combat power in 1942 and conduct large-scale offensive operations in 1943 and 1944.[116]

The Soviet Partisan movements' synergistic effects were crucial in the larger operational plans of the Soviet Red Army. Without the ability to disrupt and occupy German forces, it is quite possible that the Red Army would not have been able to gain the momentum necessary to turn the tide of the German advance and ultimately defeat the German Army during World War II. Therefore, the critical placement of the Soviet Partisan movement as a hybrid force—with its synergistic effects—provided a necessary advantage to the Red Army in achieving overall victory against the Germans.

[113] Ibid., 129-134.

[114] Ibid., 115.

[115] Ibid., 129.

[116] Zeimke 2002, 103.

4. Validation of a Theory

This monograph has set out to conclude a valid theory of hybrid warfare through a synthesis of military theory and historical trends. In doing so, a qualitative theory and several supporting principles have been identified and evaluated in relation to the two very unique historical case studies: the 2006 Israel-Lebanon War and the Soviet Partisan movement on the Eastern Front during World War II. The classic example of Lebanese Hezbollah—which generated so much discourse in the U.S. about hybrid warfare because of the surprising success of Lebanese Hezbollah against the Israeli Defense Forces in 2006—is fundamentally important to any analysis of hybrid warfare as the first recognized event of its kind. As such, Lebanese Hezbollah serves as the benchmark for all hybrid warfare examples—and any theory that attempts to capture the essence of hybrid warfare must first address this benchmark. Analysis of the Soviet Partisan case is particularly useful in that it first adds to the existing literature of hybrid warfare. Secondly, the Soviet Partisan movement occurred within the largest military conflict in the era of modern warfare—and garnered significant, measurable effects. The result of this dual analysis has been the affirmation of the proposed theory and the recognition of the qualitative presence of each of the proposed principals within the 2006 war between Israel and Lebanese Hezbollah and the Soviet Partisan movement of World War II—leading to the potential for future application of the theory to emerging threat scenarios to aid military professional understanding.

The Significant Implications of Hybrid War Theory

Many implications exist because of the validation of this theory. Perhaps the most significant result of a relevant theory is the ability to anticipate emergent hybrid organizations. Analysis of existing and emerging threat organizations can assist in the classification of threats so that regional forces can holistically understand behaviors as they emerge. This classification and understanding of behaviors then lends itself to predictive assessments of likely hybrid actions—in keeping with the proposed theory of hybrid warfare.

Specifically in the Middle East, this theory explains with some plausibility the emergence and the behavior of Lebanese Hezbollah as one of the preeminent hybrid threats today. In and of itself, this is beneficial to the U.S. and its allies as they seek to first understand and then predict Lebanese Hezbollah's actions in Lebanon, the Middle East, and the Globe. This enables military forces to understand not only the capabilities of the hybrid force, but also the motivations and likely limitations of such a force. For example, understanding Lebanese Hezbollah as a defensively oriented force motivated by a perceived existential threat alters the conventional calculus that is often used in assessing this organization. Furthermore, this understanding then allows the U.S. military forces to allocate resources and prepare contingency type responses to these potential actions. In seeking to understand these motivations and proclivities, U.S. and allied forces are more likely to encounter success as they interact with this hybrid threat organization.

Within the Pacific region, the theory of hybrid warfare might be used to actively assess and monitor emerging threats as Chinese interests and capabilities increase and the region balance of power between Asian land armies adjust. Historically, an assessment such as this could have helped to explain the Viet Cong and its relationship with the

North Vietnamese Regular Army during the Vietnam War. For SOF in particular, the theory can assist in identifying non-state actors who may be likely to seek sponsorship and access to conventional type weapon systems. In identifying these groups, actions can be taken to isolate them using all elements of national power before they emerge as truly dangerous hybrid threats.

Potential Outcomes

There are many potential outcomes from the realization of a valid theory of hybrid warfare. One of these is in terms of U.S. Army force structure. As the U.S. Army continues to define the future threat environment, this expanded understanding will be fundamental. The basic understanding that a hybrid threat will seek to gain advantage from its internally synergistic capabilities through the combination of conventional and unconventional technologies will allow the U.S. Army to build equipment and weapon systems that are competitive against conventional opponents, yet retain a level of resiliency against unconventional threats. Ad hoc examples of these types of modifications exist in terms of anti-IED electronic countermeasures that have been used in the wars in both Iraq and Afghanistan. Another example is in the basic construction of vehicles such as a V-hull of the Stryker vehicle to resist IED attacks while maintaining a premier conventional urban warfare capability in terms of troop carrying and speed. This utility in combining technological benefits in speed and lethality with survivability against irregular threats is essential to the U.S. Army's future success on the hybrid battlefield.

Another opportunity in adjusting force structure to combat hybrid threats is in focusing on the development and incorporation of technology. In this respect, technology could be developed to specifically target the fusion of hybrid capabilities. For example, although the combination of conventional and unconventional capabilities and tactics enables a synergistic advantage—the same combination also produces organizational seams between the different types of components. For example, in the case of Lebanese Hezbollah, a seam exists between the highly trained conventional type forces which utilize high-end weapon systems and the less well trained militia. This seam can be targeted and exploited by concentrating on the nodal linkages of command and communication between the different elements of the conventional and irregular force. Another seam potentially exists between the criminal elements and the military type elements of Lebanese Hezbollah that could be potentially targeted by military information support operations.[117] As such, the theory of hybrid warfare provides a solid benefit to the U.S. Army in responding to future hybrid threats.

The tactics used by U.S. Army forces can also benefit from a greater understanding of hybrid threats in many areas such as intelligence analysis and targeting. In terms of intelligence analysis, the theory provides a predictive template that can be used to baseline the analysis of a hybrid threat. For example, if a potential threat displays a tendency toward the fusion of multiple types of available assets and techniques: conventional, irregular, criminal, and terrorist, while operating under a perceived existential threat, a military intelligence analyst can apply the hybrid theory of warfare to look for the existence of other likely aspects of the hybrid threat. In this hypothetical case, the

[117] This monograph does not seek to explore the tactical, operational, or strategic seams between Lebanese Hezbollah and its state sponsors, although these seams do likely exist and are thereby targetable.

analyst can look for indicators of the presence of the other principles of hybrid warfare. This analysis could likely lead to the identification of a defensive orientation and a specific ideology which could in turn be used to develop a predicted enemy situational template. Again, the hybrid theory itself provides a basis for U.S. Army success against hybrid threats on the future battlefield.

U.S. Army doctrine can also benefit from the theory of hybrid warfare. *Army Doctrinal Publication 3.0: Unified Land Operations* predicts that hybrid threats will be a constant variable upon the future battlefield. The manual also proscribes a specific manner in which to conduct operations on this future battlefield. The manner described is the combination of combined arms maneuver to conventional, high-end military adversaries and the application of wide area security techniques against irregular force structures and environments. Through the selective application of these two techniques, U.S. Army forces can attempt to balance and eventually offset a hybrid force's advantages. Essentially, if the U.S. Army can determine the how and the why of a hybrid force's actions—through the application of hybrid warfare theory—the techniques of combined arms maneuver and wide area security can then be used to engage with and divide the conventional and unconventional aspects of the hybrid force. This division will, in essence, strip the hybrid force of its synergistic advantage and enable the specific targeting of individual elements within the hybrid force. As a result, the hybrid force will be much reduced in effectiveness and will be vulnerable to the U.S. Army's own combinations of conventional and irregular forces: SOF. This will ultimately allow U.S. forces to retain control of the rules and tempo of the battlefield.

Implications for Future Research

Although this monograph has explored and attempted to answer several questions, the process of inquiry itself has unearthed additional questions that should be explored in order to fully understand hybrid warfare. For example, as an understanding of hybrid threat formation develops, additional questions arise with regard to how long hybrid organizations exist and whether or not they actually serve as a transitory state. Frank Hoffman's research indicates that hybrid organizations may indeed only briefly emerge and exist as transitory entities. An analysis of historical examples in a long view may enable a better understanding of this question. Initial trends seem to indicate that hybrid organizations suffer one of two fates: (1) they are defeated or absorbed by conventional forces—as in the case of the Viet Cong and the Jewish Rebellion of 66 AD; or (2) they transition to more purely conventional forces over time—as in the cases of the U.S. Army as it evolved over time, and the Soviet Partisan Network as it merged into the Red Army. If this trend holds true, it may shed additional light on the problem of hybrid threats and offer predictive insight into the further evolution of hybrid organizations such as Lebanese Hezbollah—including the longevity of hybrid organizations.

Operational Approaches to Hybrid Warfare

by Major Richard Johnson

> The danger is that this kind of style, developed out of a single case, can easily outlive the situation that gave rise to it; for conditions change imperceptibly.
>
> Carl von Clausewitz, *On War*

1. Introduction

The Hezbollah fighters struck quickly, overwhelming the small truck-mounted border patrol with antitank rounds and small arms fire. But significantly, they only sought to kill the Israeli Defense Force (IDF) reservists in the second truck. Their objective that morning went far deeper than a simple guerrilla ambush; they sought captives. The four organized sections swept through the carnage and pulled Sergeant Ehud Goldwasser and Eldad Regev back through the hole in the border fence, under the cover of coordinated mortar fire. It took 45 minutes for an IDF relief force to reach the site to find them long gone, giving the fighters ample time to abscond with their prisoners through the Lebanese village of Ita a-Sha'ab. Barely another hour had passed when Hezbollah's Al Manar satellite television network lauded the successful kidnapping of two IDF soldiers, an effort to restore faith in their wider struggle to repatriate their own captured fighters.[1]

As the Israeli Air Force (IAF) prepared to destroy bridges radiating out from the area in an effort to contain the captives, the IDF organized a combined arms force with a Merkava tank to secure a vantage point on Giv'at Hadegel, a hill overlooking the village. The detachment never made it to Giv'at Hadegel, as a huge improvised explosive device (IED) rocked the Merkava, killing the crew of four. When the dismounted troops dispersed to secure the site, they came under heavy indirect fire which killed yet another soldier.[2] The night of 12 July 2006 came to a close with eight IDF soldiers killed, Goldwasser and Regev still missing. Reports circulated to the highest levels of the defense staff and government, providing a context for "belligerent declarations and hasty decisions that ultimately led to a war."[3]

The next morning, the IAF struck Hezbollah's Zelzal-1 and Fajr-3 missile positions across Lebanon, successfully destroying over half of their arsenal in 34 minutes. But therein lay the issue; the IAF could only destroy half of this arsenal of medium-range missiles, and very little could be done about the thousands of light, mobile Katyusha rockets distributed across southern Lebanon. The Hezbollah response was an unprecedented barrage of Katyushas into northern Israel that surprised the IDF in terms of

[1] Amos Harel and Avi Issacharof, *34 Days: Israel, Hezbollah, and the War in Lebanon* (New York: Palgrave Macmillan, 2008), 2-5, 11-12, 14; Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), 34-35. This account of the events on 12 July 2006 is drawn primarily from *34 Days*, due to Harel and Issacharoff's access to interviews with the IDF soldiers in the morning ambush at Report Point 105. Brigadier General Gal Hirsh, the division commander in the northern border area, had already identified this scenario as a major risk and previously requested that the reservists along the border be replaced; they were not.

[2] Harel and Issacharof, 12-13.

[3] Ibid., 15.

both volume and penetration.[4] Without a major land offensive, there was no practical way to disrupt the rocket attacks on Israeli population centers.

Over the next two weeks, Hezbollah simultaneously fired rockets to weaken Israeli political resolve, while defending against the IDF's continued incursions from well-prepared positions in southern Lebanon.[5] The IDF began to fixate on the town of Bint J'beil for its symbolic resonance within both societies. After the Israeli withdrawal from Lebanon in 2000, Hezbollah secretary general Hasan Nasrallah held a victory speech there. The IDF Chief of Staff, General Dan Halutz, sought to create a "spectacle of victory" through a raid in Bint J'beil rather than focus on a holistic disruption of the rocket threat to northern Israel's population.[6] At Bint J'beil, the IDF encountered stiff Hezbollah resistance, as both sides clashed in what was more of a meeting engagement than an IDF raid or a Hezbollah ambush. IDF veterans of the battle at Bint J'Beil hold a lasting impression of Hezbollah's capability, one that is far different from what they had trained and prepared. One paratroop officer remarked that "[t]hese were not the small sections we were familiar with…these didn't retreat from the field."[7] Another recalled later that Hezbollah "had eyes everywhere,"[8] and a third veteran of the conflict recollected "we were under constant fire, they never stopped hitting us…[y]ou can tell Hezbollah has been trained in guerrilla fighting by a real army."[9]

Throughout the short war, Hezbollah displayed the nature of a complex adaptive threat in which their combination of regular and irregular aspects created a synergistic effect, one greater than the sum of those component parts.[10] They mixed regular forces with a

[4] Harel and Issacharof, 91-93; Uri Bar-Joseph, "The Hubris of Initial Victory: The IDF and the Second Lebanon War," in *Israel and Hizbollah*, ed. Clive Jones and Sergio Catignani (London: Routledge, 2010), 156, 158-159. Although accurate in locating Hezbollah's Iranian medium-range rockets, Israeli intelligence failed to recognize that their light rocket arsenal was significantly upgraded with Syrian assistance prior to the conflict. Hezbollah's improved 122mm Katyusha rockets had an effective range of 42km instead of 20km, and they also had received new 220mm rockets with an effective range of 50km to 70km.

[5] Author's discussion with Retired IDF General Officer and Member of the Winograd Commission, 8 March 2012, Tel Aviv, Israel; Penny L. Mellies, "Hamas and Hezbollah: A Comparison of Tactics," in *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, ed. Scott C Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, 2009), 61; Cathy Sultan, *Tragedy in South Lebanon* (Minneapolis, MN: Scarletta Press, 2008), 40. As a result of this pattern of conflict which the IDF seemed powerless to stop, there were 43 civilians killed in Israel with 300,000 people displaced. In Lebanon, estimates are that 600,000 people fled as the IDF continued air strikes throughout the campaign. As for the military forces, the IDF suffered 119 killed in action while Hezbollah lost an estimated 184 based on the number of funeral processions recorded. Other sources estimate between 300 and 500 dead Hezbollah fighters.

[6] Joseph, 154, 156; Sultan, 54, 56; Harel and Issacharof, 119-120, 126-128, 136-139; Matthews, *We Were Caught Unprepared*, 45.

[7] Amos and Harel, 135.

[8] Sultan, 56. Sultan's work includes accounts from both a Hezbollah fighter and an IDF soldier who fought at Bint J'Beil. Her collection appears slightly biased against the IDF in its presentation, focusing on a magnitude of collateral damage in southern Lebanon which is disputed in other sources listed herein.

[9] Greg Myre, "Israel's Wounded Describe Surprisingly Fierce, Well-Organized and Elusive Enemy," *New York Times* (10 August 2006). Accessed at www.nytimes.com/2006/08/12/world/middleeast/ 12soldiers.html on 10 September 2011.

[10] Ralph Peters, "Lessons From Lebanon: The New Model Terrorist Army," *Armed Forces Journal* 114, no. 3 (October 2006): 39; Mellies, 52; Sultan, 53. To enable this adaptive nature, Hezbollah teams had much more autonomy than their IDF counterparts. This is a reflection of both the Iranian doctrinal influence and the entrepreneurial nature of Lebanese society. The Hezbollah fighter interviewed in *Tragedy in South Lebanon* explained "I have specific tasks, as do others in my small unit, but we work independently of others. I think this is our strength."

hierarchical, military-style command structure with the distributed nodes of an irregular force; a great majority of their fighters wore uniforms.[11] Most visibly, they employed a lethal combination of regular and irregular means, melding conventional weaponry such as anti-ship missiles, Kornet anti-tank missiles, and Katyusha rockets with improvised weaponry suited for irregular warfare such as IEDs and ambush sites.[12] But most importantly, Hezbollah combined regular and irregular behaviors in their form of warfare. They fought in many sustained battles, but also maintained an ability to disengage when it was advantageous. Furthermore, they displayed the ability to counterattack given the tactical opportunity.[13] Nasrallah's exhortation at the outset of the conflict provides a unique summarization of this change in modalities: "[y]ou wanted an open war. Let it be an open war. Your government wanted to change the rules of the game. Let the rules of the game change . . . [w]e are not a regular army, we will not fight like a regular army."[14]

Hezbollah engaged Israel in multiple domains, far beyond the jagged valleys of southern Lebanon. By using a combination of regular and irregular aspects to counter Israeli power on land, sea, air, and in the battle of international narratives, Hezbollah achieved a synergistic effect to exhaust Israel. This effort to indirectly exhaust Israel is illustrated in Hezbollah's central theme of *muqawama*, a notion of resistance which exploits Israel's sensitivities to casualties in attritional warfare.[15]

The IDF fundamentally did not disrupt Hezbollah's logic for violence in the conflict. Although the IAF was precise, air strikes failed to disrupt Hezbollah's balance in Lebanon and push it into an operational collapse.[16] The IDF found its historic advantages in tanks, aircraft, reconnaissance, and night raiding actions nearly irrelevant in 2006.[17] Additionally, Israeli politicians and strategists held a myopic view of their desired end state and could not provide an articulated framework for operations. Consequently, IDF commanders were left with an inherent tension in their operational plans. They were pulled between an end state which was not achievable without sustained land warfare, and a strategic context which would not allow sustained land warfare. Although the

[11] Stephen Biddle and Jeffrey A. Friedman, *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle Barracks, PA: Strategic Studies Institute, 2008), 45, 59; Hybrid Warfare Panel Discussion, 9 February 2012, Fort McNair, DC. The IDF was also captivated by the fact that Hezbollah established a regular system for administration, to include pay stubs.

[12] Peters, 38; Anthony Cordesman, "The Lessons of the Israeli-Lebanon War." Center for Strategic & International Studies, 43. Accessed at www.csis.org on 2 September 2011.

[13] Biddle and Friedman, 36, 39.

[14] Cordesman, 8; Robin Wright, *Dreams and Shadows* (New York: The Penguin Press, 2008), 198-199.

[15] Mellies, 53; Peters, 40, 42; Biddle and Friedman, 77. Biddle and Friedman illustrate the power of this synergistic effect; even though Hezbollah could not match the conventional capacity of other Arab militaries, they were more successful in holding terrain than the French in 1940 or the Italians in 1941.

[16] Gal Hirsch, "On Dinosaurs and Hornets—A Critical View on Moulds in Asymmetric Conflict," *The Royal United Services Institute Journal*148, no. 4 (August 2003): 4; Matthews, *We Were Caught Unprepared*, 61. Ironically, Hirsch illustrates a conceptual understanding of this very requirement in his 2003 article: "I recommend creating the strike through the operational logic described here: a simultaneous operational employment of forces, like a swarm of hornets." Accounts like *34 Days* imply that Hirsch was significantly constrained by higher headquarters' guidance during his command of the tactical and operational land maneuver in southern Lebanon.

[17] Shimon Naveh, "The Cult of Offensive Preemption," in *Between War and Peace: Dilemmas of Israeli Security*, ed. Efraim Karsh (London: Frank Cass, 1996), 172. Naveh illustrates the historical context of the IDF's presumed superiority over Arab forces in night raiding actions and complex mobile maneuvers.

IDF was able to raid several Hezbollah strong points and destroy most of their medium-range missiles, they failed to arrange these successes towards a strategic aim.[18] The IDF lacked both the theory and practice to prevail in the 2006 conflict; operationally and strategically, Hezbollah outlasted Israel.[19]

Significance

Israel's operational approach to the hybrid threat in Lebanon sparks an interesting discourse, an introspective dialogue about the applicability of the U.S. Army's doctrine and organization to defeat similar threats. To understand this, it is instructive to examine how the U.S. military applied operational art to defeat hybrid threats in previous conflicts. That historical inquiry guides the following research, lest we fall into the trap Clausewitz alludes to in this introduction's epigraph.

This is a potentially rewarding endeavor, because an adequate analysis of operational art can provide insight for future approaches to hybrid threats. There is a healthy debate about hybrid threats and the nature of hybrid warfare in American military journals and publications. Much of this discussion describes hybrid threats as nascent phenomena, citing the IDF's struggle against Hezbollah as a bellwether for future U.S. military operations. Significantly, much of this debate also focuses on an adversary's means and capabilities in hybrid war, rather than the cognitive fusion of mixed forms of warfare

[18] Author's discussion with Retired IDF General Officer and Land Warfare Analyst, 8 March 2012, Latrun, Israel; Author's discussion with Israeli Military Analyst, 8 March 2012, Tel Aviv, Israel; Author's discussion with Israeli Military Analyst, 9 March 2012, Tel Aviv, Israel; Matt M. Matthews, *Interview With BG (Ret.) Shimon Naveh* (Fort Leavenworth, KS: Combat Studies Institute Press), 4; Matthews, *We Were Caught Unprepared*, 62-64. Discussions with IDF theorists and practitioners reveal a disjointed relationship between theory, doctrine, and practice with respect to operational art in 2006. The IDF's new operational doctrine artificially conflated the theories of Effects-Based Operations (EBO) and Systemic Operational Design (SOD), resulting in what one officer deemed "a maze of words." Halutz's headquarters adopted this doctrine less than one month prior to the conflict, before it was studied and embraced by tactical echelons and the reserve forces. Shimon Naveh's interview corroborates this, contending that the IDF's operational doctrine was neither fully synthesized nor embraced as an adaptive organizational process. American assessments of the IDF generally combine the two issues; Matthews' own critique in *We Were Caught Unprepared* reflects this conflation, at one point referring to it as "the new EBO/SOD doctrine" and "this effects-based, SOD-inspired doctrine." Therefore, it is fundamentally incorrect to use the 2006 war as a sole basis for debating the utility of design methodology in conceptual planning.

[19] Ahmad Nizar Hamzeh, *In The Path of Hizbullah* (Syracuse, NY: The Syracuse University Press, 2004), 44, 46; Daniel Isaac Helmer, *Flipside of the COIN: Israel's Lebanese Incursion Between 1982—2000* (Fort Leavenworth, KS: Combat Studies Institute Press, 2007), 70-72; Sergio Catignani, *Israeli Counter-Insurgency and the Intifadas: Dilemmas of a Conventional Army* (London: Routledge, 2008) 190; Augustus Richard Norton, *Hezbollah: A Short History* (Princeton, NJ: The Princeton University Press, 2007), 136-137; Michael D. Snyder, "Information Strategies Against a Hybrid Threat" in *Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, ed. Scott C Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, 2009), 114-115; Matthews, *We Were Caught Unprepared*, 11, 19, 29, 34. As context for the preceding vignette, it is important to note several circumstances surrounding the July 2006 war. Fundamentally, Hezbollah is a jihadist organization which increasingly engages in Lebanese politics, not a political party with an armed wing for jihad. Israel used a combination of armed incursions, limited operations, and overt occupation in the same areas in southern Lebanon from 1982 to 2000, in an effort to create an operational security buffer. Hezbollah used the intervening six years to establish an extensive, modern bunker system; with security protocols in place, no fighter had knowledge of the entire structure. The IDF's focus during this time was chiefly on the Gaza Strip and West Bank, where they became proficient in short counter-terror operations at the expense of combined arms maneuver coordination, mobility, and logistics. Nasrallah did not expect the kidnappings to result in an open war against Hezbollah, so neither side was adequately prepared for the conflict when it began. Upon examining the bodies of Goldwasser and Regev once they were returned to Israel after the war, the IDF determined that they most likely died from wounds sustained in the initial ambush on 12 July.

which hybrid threats employ. A symptom of this focus on physical aspects is the projection for U.S. military equipment and capabilities, instead of a contemporary debate in terms of the doctrine and organization to counter hybrid threats in complimentary abstract domains. The U.S. Army genuinely needs advanced capabilities in the confusing environment of land warfare against a hybrid threat. However, these investments will not bear fruit if there is not a thorough range of operational approaches, broad methods that arrange these tactical gains in pursuit of strategic objectives. Technology and information dominance alone will not fuse tactics and strategy, but logical constructs that provide clarity and direction to an adaptive organization may provide this capability.

When operational art pursues strategic aims through the arrangement of tactical actions within the context of the adversary, it enables a force to defeat that adversary via positions of relative advantage. Translating these positions of military advantage into positions of political advantage enables successful conflict termination from a position of strength, rather than seeking a strategic break-even point. Theories of hybrid warfare, operational art, and historical analysis of the wars in Vietnam and Iraq illustrate several key concepts regarding sound operational approaches: they cognitively disrupt the hybrid threat's logic governing the forms of warfare it employs, they fuse tactical successes to the strategic aims within the context that led to the hybridized threat, and they avoid uniform approaches across time, space, and purpose. Future operational approaches to counter hybrid threats must adapt elements of these explanatory concepts.

Methodology

This monograph utilizes qualitative historical analysis to build understanding of American operational approaches to hybrid threats. To develop broad, explanatory fundamentals, this research and analysis does not attempt to quantify or otherwise model hybrid warfare in a predictive fashion. Sound historical analysis develops the widest possible consensus of significant experiences by collating direct observations and previous treatments on the event, so this may incorporate contradictions.[20] This is a reflection of the relative nature of historical analysis, and the lack of an objective, singular truth inherent to a specific event or campaign. Even the most rote, 'hard' sciences have limitations in the reproducibility of results for the same reason. In the complex and amorphous environment of historical hybrid warfare, this reproduction is achieved only through the virtual replicability of a narrative.[21] This monograph utilizes case studies to reproduce a narrative through the dual lenses of operational art and hybrid warfare.

The study of operational art and hybrid warfare though a historical lens has a set of inherent limitations, some of which are imposed by the nature of the research, and some of which are deliberately placed upon the analysis to bound the subject matter. The chief limitation on research is the specter of presentism, since accounts from Vietnam and Iraq do not share the same logical constructs with contemporary expressions of hybrid warfare and operational art. To bring reasonable limits on the scope of research, several constraints narrow the field of what is considered for analysis. The research focuses

[20] To aid in the development of this wide consensus, the case study analyses rely heavily on the direct observations of primary sources, and incorporate foreign sources to minimize American military bias.

[21] John Lewis Gaddis, *The Landscape of History* (New York: Oxford University Press, 2004), 9-10, 39-40, 42-43.

on the Army's historical experiences with hybrid warfare, since warfare is an activity among the population; the population lives on land and the Army is the eminent land force for sustained military operations.[22] American experiences with hybrid warfare form the subject matter for two reasons. First, there are many macro- and micro-cultural peculiarities of American institutions and military operations. Using case studies from American experiences isolates that variable to improve the application of resulting fundamentals for an American Army. Additionally, foreign campaigns such as the IDF in Lebanon or the Russians in Chechnya receive a majority of the treatments through a lens of hybrid warfare, creating a misconception that this may be a form of warfare which is unfamiliar to the U.S. Army's institutional lineage.[23] The application of operational art is analyzed rather than tactical methods or strategic considerations, since operational art is the closest expression of warfare to the underlying reason for hybrid threats: a technique of considering and arranging means to achieve a higher purpose. Finally, hybrid warfare is the subject rather than a wider survey of irregular warfare or unconventional warfare, owing to the relative vagueness and breadth of those concepts. Hybrid warfare is also broad concept, but it retains enough specificity and unique characteristics as to avail itself to discrete analysis. These deliberate constraints on the scope of the analysis provide clarity for the resulting fundamentals, but may limit their applicability in future conflicts.

In order to gain understanding and context for these fundamentals, this monograph continues with an investigation into the competing models that describe the elements of hybrid warfare. This discussion focuses on the form, function, and logic of unrestricted warfare, compound warfare, fourth generation warfare, hybrid warfare, and current U.S. Army doctrine. To develop a working model for hybrid warfare which frames the subsequent case study analyses, this inquiry evaluates the physical and cognitive traits of hybrid warfare, historical trends, and the external stimuli that drive a threat to hybridize. Likewise, the following chapter examines the theory, application, and elements of operational art. This context creates an appreciation for the application of operational art in a specific campaign or war, an operational approach. This discussion of operational art includes the underlying nature of modern warfare, and the inherent insufficiency of methods that linearize a complex process.

The case studies of the American experiences in Vietnam and Iraq illustrate the concepts of operational approaches to defeat hybrid threats with varying levels of success and adaptation. Each case study describes the threat, the nature of tactical actions and strategic objectives in the environment of hybrid warfare, and the operational approach which sought to broadly arrange them. The consequent analysis focuses on the effectiveness of the operational approach, with consideration of the cultural context, historical background, and grievances that led to the conflict and its termination. The monograph's

[22] Owing to the limited resources of this study, there are only two case studies presented. A full treatment on the subject would apply the same analytical logic to the American Revolution, the Mexican War, the Civil War, and Operation Enduring Freedom.

[23] Brian P. Fleming, *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art* (master's thesis, School of Advanced Military Studies, 2011), 7, 61; Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory* (master's thesis, School of Advanced Military Studies, 2009), iii; Sean J. McWilliams, *Hybrid War Beyond Lebanon: Lessons From the South African Campaign 1976–1989* (master's thesis, School of Advanced Military Studies, 2009), 3; Steven C. Williamson, *From Fourth Generation Warfare to Hybrid War* (master's thesis, U.S. Army War College, 2009), 29.

conclusion presents explanatory fundamentals to counter future hybrid threats based on the analysis of hybrid warfare and operational art theory, and the two case studies. Finally, it culminates with a brief assessment of the Unified Land Operations doctrine's ability to address hybrid threats with these fundamentals in mind.

2. The Nature of Hybrid Warfare: Built to Last

The Western discussion of hybrid threats and hybrid warfare spiked dramatically as the first analyses of Hezbollah emerged from Lebanon in 2006. The first widely publicized use of the term *hybrid warfare* for a military audience pre-dates that campaign in Lebanon, a speech by Lieutenant General James Mattis on 8 September 2005, which he quickly followed with an article in *Proceedings*.[24] There is an inherent tension between developing clean-cut distinctions among complex forms of warfare while retaining an appreciation of the whole phenomenon.[25] However, if the U.S. Army seeks operational approaches to counter a hybrid threat, then it requires a rich understanding of hybrid warfare's nuances as a point of departure for each incident. The following discussion deconstructs the ongoing scholarly debate in order to build context and examine hybrid warfare's physical and cognitive elements, its historical trends, and the reasons that an adversary develops a hybrid nature.

The Insufficiency of Symmetry and Statehood

The genesis of the current debate in hybrid warfare stems from an insufficient military vocabulary to describe these observed phenomena. After an intense focus on large-scale conventional conflicts during the Cold War, with episodic foci on irregular conflicts, the insufficiency of describing warfare in terms of symmetric and asymmetric enterprises surfaced. There are inherent limitations in characterizing any form of warfare as symmetric since a perceptive enemy will choose to strike at vulnerabilities instead of at strengths.[26] Although this is a key concept in most traditional Eastern theories of warfare, the Western military discussion of asymmetry advanced significantly with works such as Robert Leonhard's *The Art of Maneuver*.[27] Leonhard illustrates that even

[24] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 14; Frank Hoffman and James N. Mattis, "Future Wars: The Rise of Hybrid Wars." *Proceedings* 132 (November 2005); William J. Nemeth, *Future War and Chechnya: A Case for Hybrid Warfare* (master's thesis, U.S. Naval Postgraduate School, 2002); Erin M. Simpson, *Thinking About Modern Conflict: Hybrid Wars, Strategy, and War Aims* (paper presented to the annual meeting of the Midwest Political Science Association, 2005). Unpublished papers pre-dating Hoffman's effort include a 2002 Master's thesis by William J. Nemeth which represents the earliest scholarly work on the subject, in which the emergence of devolved hybrid societies gives rise to hybrid warfare as observed in Chechnya. Simpson's early work in the subject explores hybridity in forms of conflict, in the context of groups' strategic aims.

[25] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Phoenix, 2005), 248.

[26] Hew Strachan, "Making Strategy: Civil-Military Relations After Iraq." *Survival* 48 (Autumn, 2006): 71; Biddle and Friedman, 22.

[27] Robert T. Ames, *Sun Tzu: The Art of War* (New York: Ballantine Books, 1993), 78-80; Mao Tse-Tung, *On Guerrilla Warfare*, trans. Samuel B. Griffith (Chicago: University of Illinois Press, 1961), 25, 42.The works of Sun Tzu and Mao Tse-Tung both illustrate aspects of this concept. In a work attributed to Sun Tzu, the theorist contends that "[b]attle is one disposition trying to prevail over another" and all positions of advantage leading to this are relative in both time and space. Mao contends that within weakness there is inherent strength, and within strength there is inherent weakness; he seeks to "turn these advantages to the purpose of resisting and defeating the enemy."

conventional attacks are inherently asymmetric when they seek to defeat an enemy system by attacking them in advantageous mediums with dissimilar means.[28] Presenting the evolving appreciation for hybrid threats through the lens of symmetry can create awkward connotations, such as the current term "High-End Asymmetric Threat."[29]

Concurrently, the ongoing contraction of many domains is exposing the insufficient method of categorizing hybrid threats as state and non-state actors.[30] This simplistic categorization may lead to a superficial appreciation for their organizations, relationships, and social contexts. This is also a problematic binary choice when a hybrid threat develops in an area with no Westphalian notion of effective central governance.[31] In some instances, it may provide most of the security and social services that Western analysts normally associate with a state actor.[32] The lack of statehood or even state-sponsorship does not equate to a lack of effective organization and preparation for warfare. State sponsorship is simply a fact of life, another aspect of the strategic context rather than a requisite for a hybrid threat. The hybrid threat will seek to optimize their efficacy with or without it.[33] Alternatively, characterizing hybrid threats as categorically non-state actors in a global insurgency without an organizing function has two fundamental shortcomings. With respect to the model itself, an *insurgency* assumes that the threat is acting to overthrow, replace, or obviate the established government in a given region or society. It is a tenuous claim to argue that the social and economic reach of Western states constitutes an effective central government beyond their shores or direct military control, whether it is real or virtual.[34] Secondly, there is ample evidence that adversaries *can* organize across the traditional state boundaries in multiple domains, with coordinated planning, recruiting, funding, and arming that can result in an "undeniable strategic coherence" instead of simply a mutually beneficial convergence of aims.[35]

Furthermore, symmetry and statehood are only descriptive in nature, and an effective operational approach requires the explanatory foundation of a threat's unifying logic. With the conceptual limits of a definition rooted in symmetry and statehood in mind,

[28] Robert Leonhard, *The Art of Maneuver: Maneuver-Warfare Theory and AirLand Battle* (Novato, CA: Presidio Press, 1991), 108-111; Joseph S. Nye, *The Future of Power* (New York: Public Affairs, 2011), 34.

[29] Nathan Frier, "Hybrid Threats: Describe…Don't Define." *Small Wars Journal* (2009): 5. The term "High-End Asymmetric Threat" reflects an attempt to describe particularly well-equipped hybrid threats that spring from "functioning but unfavorable order" as opposed to discrete models of insurgency and terrorism that spring from the "absence or failure of order altogether."

[30] Fathali Moghaddam, *The New Global Insecurity* (Santa Barbara, CA: Praeger, 2010), 19-20; Author's discussion with Retired IDF General Officer and Land Warfare Analyst, 8 March 2012, Latrun, Israel. Psychologist Fathali Moghaddam asserts that this increased interconnectedness and interdependence is a result of fragmented globalization, which blurs the lines of a state / non-state dynamic and results in both collective and personal insecurity. Discussions with IDF officers regarding the 2006 war illuminate the risk in this compression of domains, in that media spreads information rapidly with minimal context.

[31] Huba Wass de Czege, "Thinking and Acting Like an Early Explorer," *Small Wars Journal* (2011): 4; Simpson, 3, 12.

[32] Erik A. Claessen, "S.W.E.T. and Blood: Essential Services in the Battle Between Insurgents and Counterinsurgents." *Military Review* (November-December 2007): 92-93.

[33] Author's discussion with Israeli Military Analyst, 8 March 2012, Tel Aviv, Israel.

[34] Raymond Ibrahim, *The Al Qaeda Reader* (New York: Doubleday, 2007), 11-14, 66-67, 271-273. Although the *perception* of this central power certainly leads to conflict within that given region or society. The body of Al Qaeda literature cited here is but one example, especially the opening "well-established facts" in their 1998 declaration of war against the United States.

[35] David Kilcullen, "Countering Global Insurgency." *Journal of Strategic Studies* 28 (2005): 605.

hybrid warfare is then *violent conflict utilizing a complex and adaptive organization of regular and irregular forces, means, and behavior across multiple domains to achieve a synergistic effect which seeks to exhaust a superior military force indirectly.*[36] This avoids characterizing hybrid warfare as asymmetric since that is not a distinguishing characteristic from other forms of warfare, and it does not typify a hybrid threat within a particular level of recognized governance since that does not inherently alter the form of warfare it can employ. Hybrid warfare is a mix of cognitive and physical elements, which adversaries employ to assert relative advantages in spite of their comparatively limited means. These dimensions differentiate hybrid warfare from strictly conventional or unconventional endeavors.

Competing Models of Mixed Forms of Warfare

Theorists describe these functional aspects of hybrid warfare with a variety of models and metaphors. As with any attempt to describe a varied and amorphous spectacle, each attempt to codify hybrid warfare takes on a focus and implication of its own. Several nuanced themes emerge that go much deeper than a simplified view which casts hybrid warfare as an anomaly where we see "militaries playing down" and "guerrillas and terrorists playing up."[37] These models in the current debate include unrestricted warfare, compound warfare, fourth generation warfare, and hybrid warfare. To understand hybrid warfare and develop a context for operational approaches to defeat them, it is instructive to examine each model on its own merits and applicability.

Unrestricted Warfare: Combinations in Multiple Domains

In 1999, Chinese Colonels Qiao Liang and Wang Xiangsui authored the essay *Unrestricted Warfare* which presents their concept of war without limits.[38] In response to an unbalanced strategic climate with fungible international rules, they describe a mode of warfare "which transcends all boundaries and limits, in short: unrestricted warfare."[39] Instead of solely seeking large-scale conventional war, which suits a powerful state's core competencies and means, they contend that the approach of the future will be an active decision to build the weapons or capabilities to fit the war.[40]

The essence of unrestricted warfare is that it is not limited to the physical, detached battlefield so the actions of war normally associated with military efforts will expand

[36] Hybrid Warfare Panel Discussion, 9 February 2012, Fort McNair, DC; Author's discussion with Retired IDF Military Intelligence Officer and Terrorism Analyst, 6 March 2012, Herzeliah, Israel. This monograph's description of hybrid warfare deliberately avoids the aspect of criminality for two reasons. Primarily, criminality depends on a corresponding characterization of legitimacy, and a hybrid threat may be engaging in what some consider criminal activity only as a means to de-legitimize governance efforts of a rival. Furthermore, it may simply be a nonstandard means of financing operations, which is entirely absent in other hybrid threat organizations. For example, Hezbollah finances a significant portion of its security operations and construction through indirectly aligned charities.

[37] Frier, 1, 8.

[38] See Liang Qiao and Xiangsui Wang, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing, 1999).

[39] Ibid., 12. Liang and Xiangsui are not the only ones to explore unrestricted warfare throughout history, but their creative and explanatory paper influences many contemporary strategic analysts, particularly hybrid warfare theorists.

[40] Ibid., 19.

across other domains such as economics and material resources, religion, culture, the environment, and information networks.[41] To break through these conventional limits of war, and the conception of multiple domains as detached and distinct entities, the authors suggest several methods: supra-national combinations of state and non-state actors, supra-domain combinations using platforms to attack across the spectrum of conflict, and supra-tier combinations to allow tactical units and small-scale means to achieve direct strategic effects.[42] Their principles to guide these methods include omni-directionality, synchrony, limited objectives, unlimited measures, asymmetry, minimal consumption, multidimensional coordination, adjustment, and control.[43]

Significantly, the authors did not assert that unrestricted warfare implies a chaotic implementation or an uncoupling from national strategic aims. Since *Unrestricted Warfare* examines strategic concepts, the authors do not examine the implementation of their theorized form of warfare on a practical level. The concepts of supra-domain methods and principle of omni-directionality are useful to understand hybrid threat behavior, but the model of unrestricted warfare does not specifically address the synergistic effect of hybrid warfare. While these methods may create simultaneous effects across multiple dimensions, they do not describe a function to link single successes to the broader strategic aims.

Compound Warfare: Unifying Distinct Forms

The simultaneous use of a regular or main force and an irregular guerrilla force against an enemy is described in the model of compound warfare.[44] The benefit of this combination is that it presumably pressures an enemy to both mass and disperse simultaneously, using both forces in a complimentary fashion in which the whole is greater than the sum of the parts.[45] The main forces in compound war will often seek to fortify themselves from definitive destruction with a safe haven or a major power ally.[46] The strength of the compound warfare model is that it accurately explains several familiar conflicts such as the American Revolution and the Peninsular War.[47]

Compound warfare's contribution to the evolution of hybrid warfare theory is that it describes a unified command of distinct forms of warfare, and the benefit of employing those forces. However, the compound warfare model describes two distinct forces on separate battlefields, only unified physically by support to one another and the scope of the conflict. Additionally, these subcomponents are either regular conventional or irregular guerrilla forces, without an inherent ability to adapt into different forms of

[41] Ibid., 118.

[42] Ibid., 181-199.

[43] Ibid., 206-216.

[44] Thomas Huber, "Compound Warfare: A Conceptual Framework," in *Compound Warfare: That Fatal Knot,* ed. Thomas M. Huber (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2002).

[45] Ibid., 2.

[46] Ibid., 3-4.

[47] For an illustrative case study, compare Huber's chapter "Compound Warfare in Spain and Naples" in *Compound Warfare: That Fatal Knot* and Phillipe Gennequin, *The Centurions versus The Hydra: French Counterinsurgency in The Peninsular War (1808–1812)* (master's thesis, U.S. Army Command and General Staff College, 2011).

warfare.[48] Compound warfare has great utility in describing most conflicts, with hybrid warfare theory describing a subset of compound warfare in which the regular and irregular forces achieve a synergistic effect.[49] Consequently, there is a limited ability to analyze some conflicts through the lens of compound warfare. One example is Vietnam, where the hybrid threat could promote subversive agrarian reforms one day and then mass for a conventional attack the next.

Fourth Generation Warfare: Protracting the Conflict for Benefit

The notion of hybrid warfare illustrating a fourth generation of warfare is deceptive. This model does not directly describe a combination of multiple forms of warfare, rather the emergence of a wholly new style of warfare.[50] Thomas X. Hammes' *The Sling and the Stone* provides the deepest analysis of this model, in which he asserts that this new generation of warfare uses all available networks to convince an enemy's strategic and political decision-makers that protracting a conflict is too costly.[51] In this model, tectonic shifts in the landscape of society resound in the ways in which states fundamentally conduct war. However, by describing these shifts as distinct changes instead of a continuum, it does not address this fourth generation of warfare in earlier eras, such as insurgency in French and British colonies or T.E. Lawrence's campaigns. As such, some analysts take issue with this concept.[52] In his conclusion, Hammes allows that fourth generation warfare represents an evolved form of insurgent tactics writ large.[53] Nevertheless, the critical insight from Fourth Generation Warfare is that deliberately protracting a conflict can aid a politically and militarily weaker opponent. This is important to the overall appreciation for irregular warfare, as is the opportunity for hybrid threats to exploit this opportunity.

Existing Hybrid Warfare Theory: The Deliberate Synergistic Effect

After the 2006 conflict in Lebanon, a cavalcade of literature on hybrid warfare and threats emerged. Some of these offered definitions of hybrid warfare that now seem almost singularly custom-fit to Hezbollah's operations in Lebanon: "[h]ighly disciplined, well trained, distributed cells can contest modern conventional forces with an admixture of guerrilla tactics and technology in densely packed urban centers."[54] The most complete treatments on the subject include *Conflict in the 21st Century: The Rise of Hybrid Wars* by concept developer Frank Hoffman in 2007, *The 2006 Lebanon Campaign and the Future of*

[48] Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, 21.

[49] Hybrid Warfare Panel Discussion, 9 February 2012, Fort McNair, DC.

[50] William S. Lind, Keith Nightengale, Johns F. Schmitt, Joseph W. Sutton, and Gary I. Wilson, "The Changing Face of War: Into the Fourth Generation," *Marine Corps Gazette* 73, no. 10 (October 1989): 23; Clayton L. Niles, *Al Qaeda and Fourth Generation Warfare as its Strategy* (master's thesis, United States Marine Corps Command and Staff College, 2008), 3-4. Within this concept, the first three generations are: Napoleonic warfare, a second evolutionary generation of warfare incorporating political, economic, social, and technical changes, and maneuver warfare. Much of this concept is attributed to the works of Thomas X. Hammes and William S. Lind.

[51] Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: MBI Publishing, 2004).

[52] Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, 19.

[53] Hammes, 2, 208.

[54] Frank Hoffman, "Lessons From Lebanon: Hezbollah and Hybrid Wars." *Foreign Policy Research Institute*, 1. Accessed at www.fpri.org on 2 September, 2011.

Warfare: Implications for Army and Defense Policy by Stephen Biddle and Jeffrey Freidman in 2008, and the compendium *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict* published by the Council for Emerging National Security Affairs in 2011. While these studies focus much of their analysis on the implications for defense apportionment and possible adaptations for the military, they provide a firm foundation for understanding hybrid warfare.

A critical insight from Biddle and Freidman is that there are several elements common to both conventional and guerrilla warfare. These include the use of delaying actions, harassing fires, concealment, dispersion, and strategic intents pursued via armed coercion.[55] Within this strategic intent lies a common underlying theme:

> . . . the actors' strategic logic does not cleanly distinguish "guerrilla" from "conventional," and "asymmetry" is properly regarded as a feature of almost all strategy rather than as a meaningful distinction between irregular and "regular" warfare.[56]

In this sense, conventional warfare and guerrilla warfare combine their inherently asymmetric approaches along a continuum, instead of in discrete alternatives for action.[57] Hoffman's succinct contention is similar; that hybrid warfare represents a deliberate synergy of approaches to target a conventionally capable force's vulnerabilities.[58]

Writings on hybrid warfare tend to describe the phenomenon in both physical and cognitive terms. In general, analysts describe both the threat itself and its means in physical terms immediately following the conflict in Lebanon, with descriptions of the cognitive qualities of hybrid warfare emerging later. Owing to the spectacular and unforeseen success of Hezbollah against the IDF, there was a natural tendency to focus on the effectiveness of high-tech equipment in the hands of an irregular force such as man-portable surface-to-air missiles, encrypted communications sets, purpose-built explosive devices, and anti-ship weapons.[59] Further analysis broadened the scope of hybrid warfare methods, and with it came the qualitative cognitive characteristics of organizational adaptation, command and control methods, and the synergistic effect of variation.[60]

Hoffman's earlier pieces on hybrid threats claimed that today's threats are more lethal so historical case studies may not be applicable.[61] However, his later published works, such as *Conflict in the 21st Century: The Rise of Hybrid Wars,* delve heavily into historical precedents as both a critique of other models and as evidence for his conclusions. Although the ever-evolving nature of warfare in general means that historical precedents will not fit neatly into our conceptions of present observations, it may be most

[55] Biddle and Friedman, 11-17.

[56] Ibid., 22-23.

[57] Ibid., 23.

[58] Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* 14.

[59] Frank Hoffman, "Preparing for Hybrid Wars." *Marine Corps Gazette* 91 (March 2007): 58; David E. Johnson, *Military Capabilities for Hybrid Warfare* (Santa Monica, CA: RAND, 2010), 3; Peters, 38; Cordesman, 18, 36, 43-48; Hoffman, "Lessons From Lebanon: Hezbollah and Hybrid Wars."

[60] Frank Hoffman, "Complex Irregular Warfare: The Next Revolution in Military Affairs." *Foreign Policy Research Institute* (Summer 2006), 398; Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* 14; John J. McCuen, "Hybrid Wars." *Military Review* (March-April 2008): 108; Biddle and Friedman, 59.

[61] "There is much to learn about history but it rarely repeats itself." Frank Hoffman, "Lessons From Lebanon: Hezbollah and Hybrid Wars."

accurate to describe hybrid warfare as simply part of the broader emerging trend of converging forms of warfare and behaviors.[62]

Hybrid warfare theory also sheds light on the reasons for which an adversary employs this form and behavior. Mattis' 2005 article asserts that the conventional overmatch of a superior military force creates a compelling logic for adversaries "to move out of the traditional mode of war and seek some niche capability or some unexpected combination of technology and tactics to gain an advantage."[63] Overwhelming military might dissuades them from fighting with strictly conventional means, and this relative advantage which Mattis highlights is critical since large militaries generally take longer to adapt and innovate due to their hierarchical organization.[64] Additionally, adversaries may choose to wage hybrid warfare since it lends itself to conduct amongst the population. This aids them in protracting conflict, which favors them in the absence of the overwhelming military end strength and capital that an opposing state may not be able to leverage in the conflict.[65]

U.S. Army Doctrine: A Threat-based Focus

With an institutional lack of joint force doctrine regarding hybrid warfare, the Army's current and emerging doctrinal publications illustrate a developing appreciation for the nature of hybrid warfare.[66] The army's logical construct for operations, *Army Doctrinal Publication 3-0: Unified Land Operations*, characterizes a hybrid threat as the most likely opponent. It defines it as "the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects." It further describes the hybrid threat as incorporating high-end capabilities traditionally associated with nation-states to exploit vulnerabilities and erode political commitment. In an acknowledgement of the ability to protract war in these circumstances, the threat will seek to wage war in more battle space and population than U.S. forces can directly control.[67]

Training Circular 7-100: Hybrid Threat provides the baseline model of enemy forces for combat training within the army. It defines and describes hybrid warfare in much the same manner as *Unified Land Operations*, with a deeper description of the force structure and behavior of hybrid threats. This manual describes an enemy's ability to achieve simultaneous effects instead of synergistic effects, which is more than an insignificant

[62] Biddle and Friedman, 77; Frank Hoffman, "The Hybrid Character of Modern Conflict" in *Hybrid Warfare and Transnational Threats: Perspectives for an Era of Persistent Conflict* (Washington, DC: CENSA, 2011), 42-45.

[63] Hoffman and Mattis, 1.

[64] Frank Hoffman, "Small Wars Revisited: The United States and Nontraditional Wars." *Journal of Strategic Studies* 28 (2005): 914; Robert M. Cassidy, "Why Great Powers Fight Small Wars Badly." *Military Review* (September-October 2002): 41.

[65] McCuen, 109.

[66] Department of Defense Joint Staff, *Irregular Warfare: Countering Irregular Threats Joint Operating Concept 2.0* (Washington, DC: Department of Defense, 2010) 9, 16. The Joint Operating Concept for Irregular Warfare only refers to hybrid warfare in a footnote, which may account for the five ways it professes to counter irregular warfare: counterterrorism, unconventional warfare, foreign internal defense, counterinsurgency, and stability operations.

[67] Headquarters, Department of the Army, *Army Doctrinal Publication 3-0: Unified Land Operations* (Washington, DC: Department of the Army, 2011), 4.

choice of terms.[68] In the discussion of hybrid threat concepts, it astutely states that opponents have difficulty isolating specific challenges within the environment, that protracted conflict favors the hybrid threat, and that the most challenging aspect may be the threat's ability to rapidly adapt and transition.[69] The discussion of hybrid threat components focuses on the nature of groups that combine, associate, or affiliate in an attempt to degrade and exhaust U.S. forces rather than cause a direct military defeat.[70] However, with much of the army currently training or conducting security force assistance and counterinsurgency operations, it remains to be seen how much of this model will take root in the force beyond the Army's combined training centers.

Summary: Understanding the Large Gray Spaces

This study's definition of hybrid warfare as violent conflict utilizing a complex and adaptive organization of regular and irregular forces, means, and behavior across multiple domains to achieve a synergistic effect which seeks to exhaust a superior military force indirectly grows from an assemblage of several different conceptualizations of hybrid warfare. First, from unrestricted warfare's tenets it incorporates omni-directional attacks across domains and the combination of means. Unrestricted warfare also describes the ability to develop capabilities to suit the environment and balance of power, which is a key component of a hybrid threat's adaptive nature and organization. From compound wars, it includes the cognitive tension created in simultaneously dispersing and massing forces to counter a hybrid threat, and the notion of nonlinear effects in combining different components. From fourth generation warfare, it integrates the evolving loss of states' monopolies on violence and the effects of protracted conflict. This is particularly useful in understanding a hybrid threat's aim of cognitively exhausting an enemy's political will to continue the conflict while physically exhausting an enemy's military combat capability.[71] Finally, from the existing concepts of hybrid warfare, it retains the central themes of a deliberate synergistic effect, the concept of forms of warfare in a continuum, and the rapid organizational adaptation of hybrid threats.

Without a strict set of classifications or bounds, this study's definition of hybrid warfare deliberately lends itself to a continuum rather than categorizations. If theory is to be useful, it must be abstract enough to account for a variety of situations yet specific enough to describe a definitive phenomenon with accuracy.[72] There are

[68] Headquarters, Department of the Army, *Training Circular 7-100: Hybrid Threat* (Washington, DC: Department of the Army, 2010), 1-2.

[69] Ibid.

[70] Ibid., 2-1.

[71] Author's discussion with Retired IDF General Officer and Member of the Winograd Commission, 8 March 2012, Tel Aviv, Israel. In this aspect, hybrid threats reveal their generic strategic disposition. The 2006 war illustrated that in the most simplistic terms, a large expeditionary force considers a stalemate a strategic loss while a hybrid threat considers a stalemate a strategic victory.

[72] Author's discussion with Retired IDF General Officer and Land Warfare Analyst, 8 March 2012, Latrun, Israel. The danger in labeling any form of warfare is that it can over-simplify the problem for the commander; there are an abundance of prescriptive theories for counterinsurgency, counterterrorism, etc. For this reason, explanatory conclusions must accompany a theory describing a certain phenomenon in warfare.

many different competing theories and models which explain hybrid warfare, but as Hoffman states:

> [i]f at the end of the day we drop the 'hybrid' term and simply gain a better understanding of the large gray space between our idealized bins and pristine Western categorizations, we will have made progress. If we educate ourselves about how to better prepare for that messy gray phenomenon and avoid the Groznys, Mogadishus and Bint Jbeils of our future, we will have taken great strides forward.[73]

This contention drives the following analysis of operational art. Existing hybrid warfare theory aptly demonstrates both the nascent nature of this form of conflict, as well as its utility against militarily superior forces. Specifically, this is done with the synergistic combination of irregular and regular qualities in protracted warfare to exhaust the superior force. Hybrid threats will emerge, and will be conceptually *built to last*. It may be impossible to completely avoid the Groznys, Mogadishus, and Bint J'beils of the future via preparation or strategic adroitness, so there must be an adequate model to guide unified action against a hybrid threat.

3. The Nature of Operational Art: Built to Outlast

Operational art is "the pursuit of strategic objectives, in whole or in part, through the arrangement of tactical actions in time, space, and purpose."[74] It creates a pathway to conflict termination in the absence of a singular decisive battle; this pathway is commonly known as a campaign.[75] Since operational art is a *pursuit* of strategic objectives instead of the *fulfillment* of strategic objectives, it implies that campaigns continue via positions of relative advantage instead of culminating and re-starting in an iterative process.

Operational art exhibits the inherent cognitive tension between tactics and strategy since the mechanical context of tactical activity blends with the abstract context of strategic thinking. Therefore, it requires a new mode of discourse beyond tactical and strategic thinking.[76] Challenges with the implementation of operational art illustrate this tension. When operations quickly arrange tactical actions in terms of purpose but are slow to implement them in terms of temporal and spatial arrangements, they may gain

[73] Frank Hoffman, "Hybrid vs. Compound War." *Armed Forces Journal Online* (2009), accessed at www.armedforcesjournal.com on 2 September 2011.

[74] Headquarters, Department of the Army, *Army Doctrinal Publication 3-0: Unified Land Operations*, 9. Michael J. Brennan and Justin Kelly, *Alien: How Operational Art Devoured Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2009). This monograph focuses on operational art instead of the amorphous 'operational level of war' which has a potential to subsume strategic concerns in military operations. All of the 'levels of war'(tactical, operational, and strategic) are logical constructs which aid in organizing military actions and concepts, but this monograph will analyze the more specific sets of tactical actions, strategic aims, and the operational art which links them. For a deeper discussion on this subject and the viability of an 'operational level of war,' refer to Brennan and Kelly.

[75] Michael J. Brennan and Justin Kelly, "The Leavenworth Heresy and the Perversion of Operational Art." *Joint Forces Quarterly* 56 (1st Quarter 2010): 112.

[76] Shimon Naveh, *In Pursuit of Military Excellence* (London: Frank Cass Publishing, 1997), 6-7; Huba Wass de Czege, "Operational Art: Continually Making Two Kinds of Choice in Harmony While Learning and Adapting." *Army* 61 (September 2011): 54-55. Although, the strategic aims of war should include an *appreciation* for the limits of mechanical tactical means in war, as the tactical actions in war should include an *understanding* of the abstract strategic environment.

no relative advantage.[77] In terms of cognitive and physical aspects, the challenges and apparent differences in the strategic, operational, and tactical activities in war may lead to their stratification in many doctrinal models for warfare. Proper doctrine should link all three through the conduit of operational art.[78] The hierarchical separation of a continuum of three levels of war is a helpful but artificial system, which doctrinaires construct to nest concepts in war.[79] While arranging tactical actions, operational art must provide a conduit to incorporate the impact on strategic context, lest decision-makers become disconnected sponsors of war.[80]

The Characteristics of Operational Art: Blending Grammars

Operational art must consider the conflict's environmental context in order to provide this conduit between tactical actions and strategic aims. In this, several elements of Western and Eastern thought manifest themselves. A Western approach sets up an ideal form (an *eidos*) which translates directly to a goal (a *telos*), and then seeks action to make this a reality. This goal constitutes a theory for action, which is put into practice. As such, theory and practice are for all intents coupled into theory-practice. However, this theory-practice by itself is insufficient since warfare is an activity that lives and reacts.[81] An Eastern approach relies on the inherent potential of a situation, instead of projecting a plan borne strictly of theory-practice. It is an attempt to use the situational context to gain a relative advantage through its inherent propensity.[82] Operational art illustrates this notion in its elements of "setting conditions" and "shaping operations."[83] This has particular importance concerning hybrid threats, since these threats tend to destabilize familiar forms and contexts for a military force.[84]

An operational approach is the cognitive *method* of arranging tactical actions in time, space, and purpose in pursuit of strategic aims; it is the application of the elements of operational art within a specific context. Culture exerts a great influence on the cognitive methods initially available to fuse tactics and strategy. A military's organizational doctrine, shared experiences, capabilities, and constraints combine to provide a starting point for operational art. Efforts to understand the environment and provide a rich

[77] Frans P.B. Osinga, *Science, Strategy, and War: The Strategic Theory of John Boyd* (London: Routledge, 2007), 236. Osinga's commentary on John Boyd's theories describes this in terms of "tempo."

[78] Brennan and Kelly, "The Leavenworth Heresy and the Perversion of Operational Art," 114. Major Leighton Anglin suggested the metaphor of a "conduit" in a discussion with the author, 22 July 2011. This is a further reflection of the fusing of tactical actions, operational art, and strategic aims rather than separate, stratified levels of warfare.

[79] Brennan and Kelly, "The Leavenworth Heresy and the Perversion of Operational Art," 114; Wass de Czege, "Thinking and Acting Like an Early Explorer," 1-2, 4.

[80] Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War." *International Security* 17 (1992):, 89; Brennan and Kelly, "The Leavenworth Heresy and the Perversion of Operational Art," 115.

[81] Francois Jullien, *A Treatise on Efficacy: Between Western and Chinese* Thinking, trans. Janet Lloyd (Honolulu, HI: University of Hawai'i Press, 2004), 1, 3, 14. Jullien traces the Western lineage of thought to Greek philosophers, hence the usage of *eidos* and *telos* to illustrate the concepts of Western thought.

[82] Ibid., 16, 21. Jullien states that "[p]otential consists of determining the circumstances with a view to profiting from them."

[83] Headquarters, Department of the Army, *Army Doctrinal Publication 3-0: Unified Land Operations*, 12-13. Unified Land Operations doctrine describes Decisive, Shaping, and Sustaining operations as part of the operational framework.

[84] Hirsch, 2.

frame for problem solving can assist operational planners in developing approaches that are refined for a specific context. Antulio J. Echevarria describes this with the metaphor of grammar when he examines the U.S. Army's struggle to adapt familiar conventional operational approaches to counterinsurgency efforts after decades of a focus on conventional warfare. He describes the two forms of warfare as having the same logic but distinct grammars, with the contemporary nature of warfare requiring the mastery of both grammars.[85] It follows that hybrid warfare requires the *blending* of both grammars.

The Theoretical Lineage of Operational Art

To understand when operational art began as a method to fuse tactical action and strategic aims, it requires an examination of when operational maneuver began. The Napoleonic wars of the early 19th century showed the first hints of operational maneuver, and the art and science requisite to employ it, but movement was still the means to arrive on a set battlefield in a position of advantage.[86] This was a result of the dominant theories of warfare at a time, which focused on the concept of a concentrated force defeating a larger dispersed force to achieve a decisive victory. However, these wars showed the utility of commanding distributed forces and arranging the continuous actions of a campaign in space and time.[87] The increased accuracy and lethality of direct fire weapons during the 19th century atomized the battlefield, and the expansion of railroads and telegraph links enabled both large-scale transport and communication over long distances. The effects of these technological advances were evident in the American Civil War, which was arguably the first comprehensive use of operational art. Dispersed elements could now fight in synchrony over great distances, requiring commanders to arrange their actions in time, space, and purpose.[88]

On the heels of the Napoleonic era, Prussian officer and educator Carl von Clausewitz labored to complete a comprehensive theory of war in relation to policy, and its resulting implementation in warfare.[89] In a departure from the Enlightenment era military theories of the time that contained fixed values and prescriptive principles for winning wars, he focuses on the inherent uncertainty in war. Because he sees decisive victory as a function of strategy, tactical battles alone could not achieve victory for an army in the field.[90] Within *On War*, Clausewitz's description of the nonlinear aspect

[85] Antulio J. Echevarria II, "American Operational Art, 1917–2008," in *The Evolution of Operational Art,* eds. Martin Van Creveld and John Andreas Olsen (Oxford, UK: The Oxford University Press, 2011), 137, 161.

[86] Michael R. Matheny, *Carrying the War to the Enemy: American Operational Art to 1945* (Norman, OK: University of Oklahoma Press, 2011), 4-9.

[87] James J. Schneider, *Vulcan's Anvil: The American Civil War and the Foundations of Operational Art* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2004), 2, 26, 30.

[88] Ibid., 17, 33-35.

[89] Carl von Clausewitz, *On War,* trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 24-25, 65-67; Matheny, 9. Significantly, Clausewitz died in 1832 before *On War* was complete to his satisfaction and must be studied with this fact in mind. As a result, some of the grander concepts that lead his work were not completely reconciled with discussions on operations and tactics later in *On War.* An additional hindrance for modern readers is Clausewitz's use of the term *strategy* to describe grand strategy, theater-level military strategic, and operational art; his use of the term must be considered in the context for each usage in *On War.*

[90] Antulio J. Echevarria II, *Clausewitz and Contemporary War* (Oxford, UK: Oxford University Press, 2007), 141-142, 145; Clausewitz, 227-229, 236-237, 263-270.

of warfare and his Center of Gravity construct shape much of the modern conceptions of operational art.

Although *On War* predates most of the mathematical concepts of nonlinearity by more than a century, Clausewitz's description of the *friction* of war shows an intuitive sense of this phenomenon. The friction of war illustrates the small details in warfare that have macroscopic effects, leading to a cumulative unpredictability due to their interconnected relationships.[91] Clausewitz rejects the clockwork nature of his contemporary military doctrines because they failed to address the cumulative effects of the dynamic processes, feedbacks, and friction that the Enlightenment's linear systems professed. Therefore, distributed command models such as *Aufstragtaktik* and mission command are logical responses, since they distribute uncertainty and allow smaller forces to make adjustments within their local context.[92] Clausewitz's other chief contribution to operational art is the Center of Gravity construct. He describes the Center of Gravity as "the hub of all power and movement, on which everything depends," and striking it theoretically leads to decisive victory.[93] Clausewitz's Center of Gravity refers less to the physical concentration of strength, and more to the forces that concentrate it. Furthermore, his Center of Gravity model is a complex phenomenon that relies on the relationship between both belligerents. Much like the spatial movement of the center of gravity of two grapplers as they struggle for a dominant position, a Clausewitzian Center of Gravity displays cognitive movement as both sides maneuver in battle. As a result, it is paramount to identify the unifying force in an adversary's system within the context that leads to its construction, and understand one's own impact on this system and the environment.[94] These aspects of the Center of Gravity are critical in operational approaches to defeat hybrid threats since they avail the possibility to define and strike ideological, political, and economic sources.[95]

Another intellectual ancestor of current operational art is the theory of Deep Battle, developed through the works of Soviet theorists such as A.A. Svechin, M.N. Tukhachevsky, and G.S. Isserson after World War I.[96] In an effort to restore mobility and operational maneuver to the battlefield, Deep Battle sought to break the physically linear aspect of an enemy front with simultaneity and depth in a focused area.[97] Isserson's theories also

[91] Clausewitz, 119-121, 139-140; Beyerchen, 73, 77.

[92] Antoine Bousquet, *The Scientific Way of War: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 87, 89-90.

[93] Clausewitz, 595-596; Echevarria II, *Clausewitz and Contemporary War*, 179.

[94] Clausewitz, 485-487, 597; Echevarria II, *Clausewitz and Contemporary War*, 180.

[95] Werner Hahlweg, "Clausewitz and Guerrilla Warfare" in *Clausewitz and Modern Strategy*, ed. Michael Handel (London: Frank Cass, 1986), 128-131; Peter Paret, *The Cognitive Challenge of War* (Princeton, NJ: The Princeton University Press, 2009), 97-99; Christopher Daase, "Clausewitz and Small Wars" in *Clausewitz in the Twenty-First Century*, eds. Hew Strachan and Andreas Herberg-Rothe (Oxford, UK: The Oxford University Press, 2007), 183; Clausewitz, 479-483. Although *On War* has little focus on irregular warfare as we would recognize it today, his earlier lectures on small wars (*Kleinkrieg*) and guerilla warfare (*Volkskreig*) are integrated into his short passage "The People in Arms."

[96] Jacob W. Kipp, "The Tsarist and Soviet Operational Art" in *The Evolution of Operational Art*, eds. Martin Van Creveld and John Andreas Olsen (Oxford, UK: The Oxford University Press, 2011); G.S. Isserson, *The Evolution of Operational Art*, trans. Bruce W. Menning (Fort Leavenworth, KS: U.S. Army School of Advances Military Studies, 2005); Aleksandr A. Svechin, *Strategy*, ed. Kent D. Lee (Minneapolis, MN: East View Publications, 1992), 217-256.

[97] Richard W. Harrison, *Architect of Soviet Victory: The Life and Theories of G.S. Isserson* (Jefferson, NC: McFarland and Company, 2010), 76-78. USSR Commissariat of Defense, *Field Service Regulations Soviet Army 1936*, trans. Charles Borman (Washington, DC: The Army War College, 1937), 1-2, 59-61; Isserson, 49.

build on Clausewitz's concept of culmination, and the attempt to attain objectives before exhausting combat power.[98] This takes advantage of the continued spatial growth of the physical battlefield, as well as the increased mobility for motorized and mechanized forces. Deep Battle and the experience of World War II illustrates the need to integrate operational art in separate domains.[99] As a result, mass and maneuver became unifying concepts to arrange tactical actions in operational art. The U.S. Army's AirLand Battle doctrine furthered this trend of abstraction and integration, describing a unifying concept of securing or retaining the initiative in order to apply combat power.[100]

Maintaining the initiative through relative advantages provides the central theme for current U.S. Army doctrine, organized in the model of Unified Land Operations. This model organizes the enduring concepts that describe a land force which seizes, retains, and exploits the initiative in order to set the conditions favorable for conflict resolution and termination.[101] These efforts are executed through decisive action, by the means of combined arms maneuver (CAM) and wide area security (WAS), and guided by mission command. Decisive action illustrates that forces employ simultaneous combinations of offensive, defensive, and support operations. CAM and WAS provide the twin means to apply combat power to these combinations. The two are complementary; CAM provides the means to seize and exploit the initiative whereas WAS provides the means to retain the initiative. Both are cognitive approaches that are not meant to be employed in isolation.[102] To adapt Echevarria's metaphor of logic and grammar, maneuver is the logic that connects the distinct but complimentary grammars of CAM and WAS. In Unified Land Operations, operational art provides the cognitive links in this structure, serving as the conduit between tactical actions and strategic aims. It stresses the importance of context for operational art, stating that it requires commanders who "continually seek to expand and refine their understanding and are not bound by preconceived notions of solutions."[103]

Operational Art and the Nature of Warfare

The evolution of operational art highlights the development of the battlefield from one with linear arrangements of time, space, and purpose, to a more fluid and dynamic environment. Although an observer would have little difficulty noting the different environments of a Napoleonic battlefield and southern Lebanon in 2006, practitioners of operational art must take special care with the subtle difference between complicated warfare and complex warfare. Complicated systems may have a dizzying multitude of one-to-one relationships, but they display linear phenomena such as additivity, which allows modeling and prediction. Complex systems with interconnected relationships do not obey the principle of additivity, so two nearly identical initial conditions can result

[98] USSR Commissariat of Defense, 1-2, 7; Harrison, 69, 149.

[99] Isserson, 150; Harrison, 98.

[100] Richard M. Swain, "Filling the Void: The Operational Art and the U.S. Army." in *Operational Art: Developments in the Theory of War*, eds. B.J.C. McKercher and Michael Hennessy (Westport, CT: Praeger, 1996), 159; Headquarters, Department of the Army, *Field Manual100-5:Operations* (Washington, DC: Department of the Army, 1986), 14-16.

[101] Headquarters, Department of the Army, *Army Doctrinal Publication 3-0: Unified Land Operations*, 1.

[102] Ibid., 5-6.

[103] Ibid., 10.

in vastly different outcomes.[104] Several aspects of operational art must be examined though the lens of complexity due to the friction of war and its inherent instability.[105]

First, technical superiority is not a substitute for a sound operational approach. A metaphoric silver bullet may lend a measurable and absolute advantage in a linear system, such as the use of the longbow at Crecy. However, this only lends a relative advantage in a complex system, which may be negligible.[106] The complexity of modern warfare also tends to marginalize the capabilities of over-centralized command and control networks. Too many interconnections may be a hindrance if units lose their ability to act independently.[107] By providing focus through a clear and common aim, operational art can arrange the purpose of tactical actions without this tether to a central node. Secondly, the approach of attrition warfare has its limitations in a complex environment. Much like the effect of technical superiority, the assumption that a specific amount of additional combat power will result in a commensurate amount of enemy casualties assumes a constant, linear ratio.[108] An operational approach cannot simply increase friendly combat power or protect against an enemy's capability, nor can it solely fixate on linear measures of effectiveness such as body counts or the spatial range of essential services.

Summary: The Operational Approach

The characteristics and history of operational art illustrate that stability and adaptability are not antithetical in doctrine. In order to ensure a shared orientation of forces, the doctrine of operational art provides a stable framework and a common lexicon. An operational approach is the adapted implementation of this doctrine, when it is set contextually to fuse tactical actions and strategic aims. Due to the complex nature of warfare, an operational approach must evolve with the uncertain and changing nature of warfare.[109] Unless an army fights the same war in succession or the nature of warfare is unchanging, linear prescriptive theories generally do not win wars on their own merits. Conversely, the pragmatic application of broad fundamentals may enable success.

However, this application of broad fundamentals must pursue a continual strategic advantage instead of collection of sporadic victories.[110] Hybrid threats will undoubtedly form with the intent of being *built to last*, as described in the preceding chapter. As the following case studies illustrate, an operational approach with a myopic view of the end state may not adequately defeat or obviate a hybrid threat. This aspect of operational planning, providing for continuation rather than culmination, should engender an operational approach to hybrid warfare which is *built to outlast*.

---

[104] Linda P. Beckerman, *The Non-Linear Dynamics of War* (Science Applications International Corporation), section 6.2. Author's discussion with Israeli Military Analyst, 9 March 2012, Tel Aviv, Israel. One example of this concept for interconnected warfare is revealed in the off-handed Israeli description of the 2006 war as "our northern system."

[105] Beyerchen, 62, 80.

[106] Beckerman, section 1.5.

[107] Ibid., section 5.6.

[108] Ibid., section 6.2.

[109] Ibid., Conclusions.

[110] Everett Carl Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005), 3-4. Dolman highlights this inherent tension in operational art, that strategy requires continual positions of relative advantage while tactics that use decisive efforts require a culmination and reconsolidation.

The operational approach describes "the gap" between the observed state and the desired end state in a conflict of hybrid warfare.[111] In its barest theoretical form, applying operational art should be the same *action* every time: the pursuit of an objective through the arrangement of tactical actions. But historical analyses of Vietnam and Operation Iraqi Freedom (OIF) shed light on the peculiarities of this action, since the form and function of the strategic objective, tactical actions, the opposing forces, and the environment all change dramatically with each application. That is why this study focuses on an operational approach—the broad and episodic adaptation of operational art doctrine in a specific context. On the path to explanatory fundamentals, these case studies provide context to the preceding abstractions on hybrid warfare and operational art.

4. The American Experience in Vietnam: The Bull and the Toreador

> The U.S. fought the war as a bull fights the toreador's cape, not the toreador himself.
>
> – Norman B. Hannah, *The Key to Failure: Laos and the Vietnam War*

Against the backdrop of the Cold War, some regional conflicts gave rise to hybrid threats as subversions turned into increasingly violent propositions. In Indochina, Communist forces protracted the conflict and enticed the combined American and Vietnamese effort to adopt a security-oriented approach. Much like the bull in a bullfight, the American effort did not fall prey to the object of its focus. It fell to the unknown force behind the cape after succumbing to exhaustion.

The Context of Conflict in Vietnam

The Vietnam War is difficult to place in a historical context owing to the nature of the conflict itself.[112] American leaders, and to some extent the government of South Vietnam itself, fundamentally misread the conflict in terms of military security while the Communist forces cast it as a complete social revolution.[113] Beyond a competition in governments, the conflict displayed several schisms which led to grievances along urban-agrarian social fault lines, colonial and nationalist tensions, and even traces of religious conflict as the French-empowered Catholic minority gravitated toward the regime in Saigon.

Terrain and demographics also conspired to make this a demanding environment for conflict. Roughly the size of Florida with 1,500 miles of coastline, South Vietnam (SVN)

[111] Headquarters, Department of the Army, *Field Manual 5-0: The Operations Process (Incl. Change 1)* (Washington, DC: Department of the Army, 2011), p. 3-1. Army doctrine further describes the operational approach as "a broad conceptualization of the general actions that will produce the conditions that define the desired end state….[it] provides the logic that underpins the unique combinations of tasks required to achieve the desired end state."

[112] Richard B. Johnson, The Biggest Stick: The Employment of Artillery Units in Counterinsurgency (master's thesis, U.S. Army Command and General Staff College, 2011), 88-163. This section on *Context* draws heavily on the author's original work while researching the employment of artillery units in counterinsurgency operations. It is intended as a brief overview of the cultural, historical and strategic context, not an exhaustive treatment on the roots of conflict in Vietnam.

[113] Jeffery Race, *War Comes to Long An* (Berkley, CA: University of California Press, 1972), 151.

rapidly transitions from an open coast to a rugged central highlands with peaks up to 8,000 feet.[114] The distances between the coast and borders with Laos and Cambodia are only 30 to 100 miles, providing effective and varied infiltration routes towards the prized coastal cities. While these central highlands are sparsely populated, Saigon dominates the fertile Mekong Delta region to the south.[115] Census data from 1960 reveals the ethnic and religious divisions in the country. Of an estimated population of 15 million, tribal minorities in the central highlands such as the Montagnards accounted for roughly 1 million citizens, with a remaining 15 percent minority of Khmer (Cambodian) and Chinese.[116] Religiously, 12 million self-identified as Buddhists compared to 2 million Catholics and small minority communities of Cao Dai and Hoa Hao adherents from the remote regions of the Mekong Delta.[117]

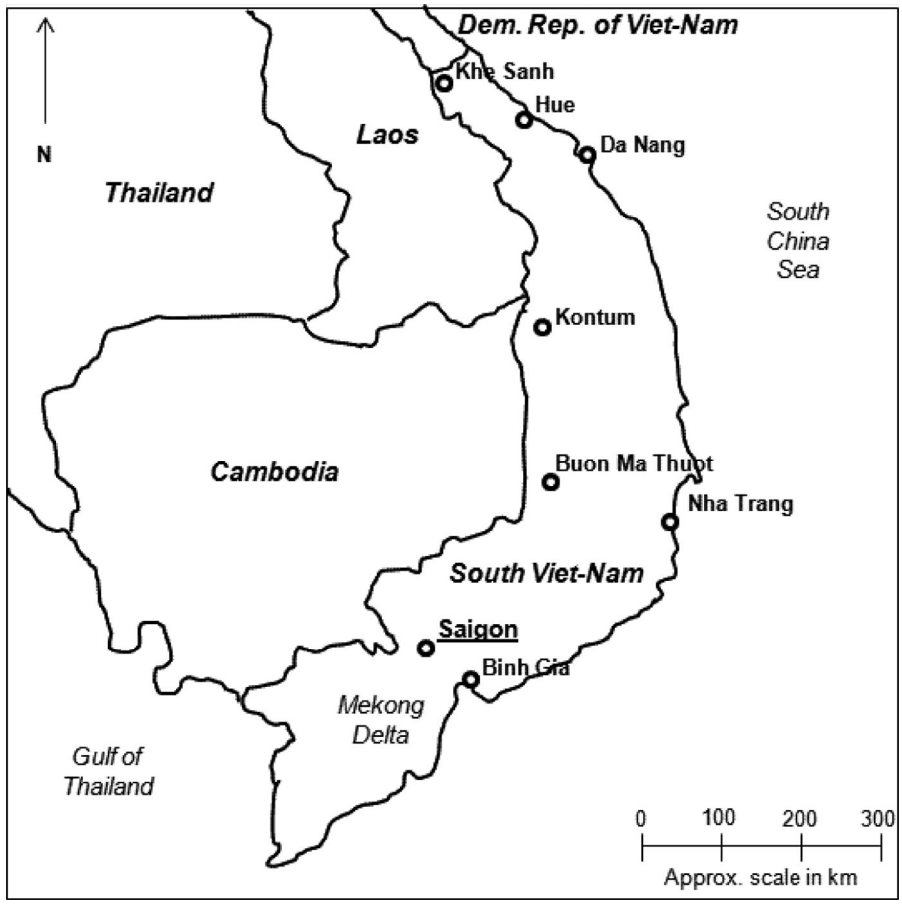


Figure 1. South Viet-Nam, 1965

[114] Ngo Quang Truong, *Indochina Monographs: Territorial Forces* (Washington, DC: U.S. Army Center for Military History, 1981), 9.

[115] Ngo, 10-11.

[116] Bernard Fall, *The Two Vietnams* (New York: Praeger, 1967), 6.

[117] William C. Westmoreland, *A Soldier Reports* (New York: Da Capo Press, 1976), 52.

Historically, Vietnam had French colonial administration and nominal rule from the 19th century until the Japanese swiftly destroyed French presence in 1944.[118] The *Viet Minh* began as a resistance force to Japanese occupation, supported by both Chinese nationalist advisors and American Office of Strategic Studies teams.[119] This endowed them with considerable experience and organizational structure, which prepared them for the political chaos ensuing Japan's surrender in 1945. Chinese, British and American advisors, liberated French prisoners of war, and the *Viet Minh* all struggled to establish effective governance in Vietnam.[120] The Vietnamese held an ingrained distinction between northern and southern societies, but the emerging paradigm in the re-established French colonial administration resembled an urban-rural division for the first time.[121] After nearly a decade of counterinsurgency, French airborne units established a lodgment in order to extend their operational reach into Laos and interdict key *Viet Minh* routes. In what would come to be known as the siege of Dien Bien Phu, *Viet Minh* forces defeated the French garrison and prompted the eventual transition to Vietnamese rule.[122]

By 1954, the United States had already begun to send military assistance directly to the provisional governments in Indochina rather than the remaining French apparatus. This support was formalized in the Military Assistance Advisory Group (MAAG), which utilized a Korean War model to equip and train conventional units in an assembly-line fashion.[123] And by 1960, it was apparent that this model was insufficient to meet the threat of hyper-organized communist subversion and terrorism. Assassinations and targeted killings rose to over 4,000, and massed troops infiltrated to Kontum and other ill-equipped army garrisons.[124] In 1962, the Joint Chiefs of Staff superseded MAAG with an expanded mission to coordinate all American security activities within SVN, the Military Assistance Command—Vietnam (MACV).

[118] Fall, *The Two Vietnams*, 54. During the early years of World War II, the Japanese allowed the sustained administration of French Indochina by an overseas government loyal to the Vichy French, and this uneasy setup lasted until the liberation of metropolitan France by Allied forces.

[119] Ibid., 67.

[120] Fall, *The Two Vietnams*, 68-71; Bernard Fall, *Hell in a Very Small Place* (Philadelphia: Lippincot Press, 1966), 23.

[121] Fall, *The Two Vietnams*, 13, 78.This is partially a reflection of the Vietnamese expansion from their ethnic northern base in a southward colonial fashion, concurrent with the start of European competition in Asia.

[122] Vo Nguyen Giap, *Inside the Vietminh: Vo Nguyen Giap on Guerrilla War* (Quantico, VA: Marine Corps Association, 1962), chapter 4; Fall, *Hell in a Very Small Place*, 482. Giap's account of Dien Bien Phu is an excellent self-examination of the strengths and liabilities inherent to his style of guerrilla warfare. Although it has some tones of Marxist exhortation, it maintains a seemingly objective view towards the military aspects of the campaign. French officers and historians rightly view this as a defeat, not a surrender.

[123] Fall, *The Two Vietnams*, 318-320.

[124] Bernard Fall, *Street Without Joy* (New York: Shocken Books, 1961), 345.

Early American efforts to address security and pacification include the failed Strategic Hamlet program,[125] expanded advisory efforts,[126] and prompting the Diem regime in Saigon to invest in paramilitary Territorial Forces.[127] Intelligence estimates and local leaders' intuition in 1964 indicated that some areas were transitioning to a phase of mobile warfare, prompting a presidential decision to enlarge MACV's force by 44 battalions in 1965.[128] It was in this new phase of operations that MACV would need to arrange tactical actions and unifying themes in SVN to pursue the strategic aim of creating a secure, western-aligned state.

The Hybrid Threat in Vietnam: Dau Tranh

The hybrid threat in SVN was an admixture of regular and irregular modes. Although certain facets of the threat appeared uniform in nature, the overall organization was both complex and adaptive. Furthermore, it displayed an amalgam of regular and irregular forces, means, and behaviors.[129]

Communist forces were a complex organization, since the sum of their component elements achieved far greater effects than a simple linear aggregate of combat power. This is a reflection of their concept of victory: a decisive superiority in the balance of forces

[125] Robert Thompson, *Defeating Communist Insurgency* (London: Chatto and Windus, 1966), 121-140; Robert Thompson, *No Exit From Vietnam*. (New York: Davis McKay Company, 1969), 169-170; Mark Moyar, *Triumph Forsaken* (New York: Cambridge University Press, 2006), 156-159; Robert Komer, *Bureaucracy at War: U.S. Performance in the Vietnam Conflict* (Boulder, CO: Westview Press, 1986), 138; Fall, *Street Without Joy*, 363. The Strategic Hamlet program was an effort to extend governance to the countryside and provide a local counter-organization to the VC, with theoretical roots in the Malayan Emergency. The execution and scope of the Strategic Hamlet program was uneven; it did not enjoy initial support from MACV, did not incorporate enough local security, and it began hastily in regions with nepotistic connections to the Diem regime. The VC viewed this as an opportunity to insert an intelligence network into the villages themselves. In any case, the sudden collapse of the Diem regime effectively terminated the program. The Strategic Hamlet program failed to achieve any cohesive effect, and at its conclusion in 1963 there were an estimated 23 VC battalions operating in the Mekong Delta, the very region where the program was initiated.

[126] Westmoreland, *A Soldier Reports*, 56, 67-68. The effort in SVN counted 16,000 advisors by January 1964. Through prior command relationships and mentorship between Westmoreland and Ambassador Maxwell Taylor, Westmoreland effectively served as a deputy ambassador for military affairs.

[127] Ngo, 26, 96. Formalized in 1961, the GVN eventually organized these territorial forces into Regional Forces (RFs) and Popular Forces (PFs) in 1964. This gave the GVN a force to fight an insurgency that had grown from a "brush fire subversion," since they had to focus the conventional forces of ARVN along the border. RFs constituted a military force at the disposal of a district-level or provincial-level leader, while the PFs served a military function for local security in individual villages.

[128] Edward Lansdale, "Contradictions in Military Culture" in *The Lessons of Vietnam*, ed. W. Scott Thompson and Donaldson Frizzell (New York: Crane, Russak and Company, 1977), 45; Moyar, 412-416. As 1965 approached, General William C. Westmoreland (Commander, MACV) and his staff realized that the disjointed strategy of defending large bases to bomb military targets in North Vietnam was having minimal effect within SVN itself. The initial plan for 68 battalions was intended to "halt the losing trend," with pacification remaining the responsibility of ARVN forces.

[129] Truong Nhu Tang, *A Viet Cong Memoir* (San Diego, CA: Harcourt-Brace Jovanovich, 1985), 130-140, 169. A note on terminology: different scholarly works assign different labels to elements of the hybrid threat in Vietnam. The People's Army of Vietnam (PAVN) of the DRV appears as the North Vietnamese Army (NVA) in most texts referred to in this monograph. As such, this is the label assigned to the conventional forces operating under guidance from the Central Office for South Vietnam (COSVN). Similarly, for southern or regrouped Communist forces under the guidance of the National Liberation Front (NLF), the label Vietcong (VC) appears more frequently than the official People's Liberation Armed Forces (PLAF). Although the term VC was a pejorative for any Vietnamese Communist (*viet nam cong san*), it is the most recognizable in applicable literature.

for a given area. This balance of forces referred to a ratio of resultant political power, not military capability.[130] In one sense, this purposeful organization mattered as much as tactics and ideology, since the aim was neither the defeat of the Army of the Republic of Vietnam (ARVN) nor the occupation of territory. The aim was an organization in depth of the population, a victory by both organizational method and means.[131] The National Liberation Front (NLF) had southern Communist forces of the *Viet Cong* (VC) that functioned as self-sufficient elements for subversion and limited security actions, whereas North Vietnamese Army (NVA) elements in SVN exhibited a more traditional hierarchical structure and method.[132] Originally, the NLF incorporated many nationalist non-Communist groups, but these groups' influence waned as the Democratic Republic of Vietnam (DRV) gained influence and overt guidance. The Central Office for South Vietnam (COSVN) embodied this degree of control linked to Hanoi.[133]

The threat organization was also adaptive, illustrated in Giap's application of the *dau tranh* theory of warfare. This theory, based on the three stages in a Maoist model of warfare, allowed forces to gradually develop and adapt in a protracted struggle based on local conditions.[134] Communist forces were inherently local and decentralized, whereas the Government of South Vietnam (GVN) forces were district-minded and rigidly centralized. This allowed Communist forces to raise recruits and money through both attractive and coercive policies at the local level, since they viewed the village leaders as the critical link between the people and the party.[135] Although there was always a degree of political and social tension between COSVN and the NLF, Vietnamese military history now confirms that many times VC forces came under direct COSVN operational control and leadership when it was prudent, allowing these forces to adapt during transitions between the phases of warfare.[136]

[130] Race, 142-149.

[131] Douglas Pike, *PAVN: People's Army of Vietnam* (Novato, CA: Da Capo Press, 1986), 220; Douglas Pike, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam* (Cambridge, MA: The MIT Press, 1966), 111.

[132] Douglas Pike, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam* (Cambridge, MA: The MIT Press, 1966), 236-237. Of note, many of these VC soldiers and supporters regrouped to the north in the aftermath of the 1954 partition, which meant they had to be re-introduced to SVN.

[133] Truong Nhu Tang, *A Viet Cong Memoir* (San Diego, CA: Harcourt-Brace Jovanovich, 1985), 130-133.

[134] Mao Tse-Tung, *On Guerrilla Warfare* (Chicago: University of Illinois Press, 1961) translated by William B. Griffith, 54-55; Mao Tse-Tung, *The Selected Writings of Mao Tse-Tung* (Peking: Foreign Language Press, 1972), 210-214; Douglas Pike, *PAVN: People's Army of Vietnam* (Novato, CA: Da Capo Press, 1986), 223. Mao's model of protracted warfare describes three phases of warfare. The first phase is the development of political movement and limited guerilla operations controlled by the party. The second phase is a transition to full-scale guerilla warfare, and is viewed as a strategic stalemate which can last the longest time. In this phase, the force establishes base areas and uses dispersion to entice the enemy force into fruitless search-and-destroy operations. In the third phase, guerrillas supplement conventional units in open warfare (both mobile and positional battles), although Mao does not intend for a huge leap between the approaches in the second and third phases.

[135] Race, 159-161.

[136] The Military History Institute of Vietnam, *Victory in Vietnam: The Official History of the People's Army of Vietnam, 1954–1975* (Lawrence, KS: University of Kansas Press, 2002) trans Merle K. Pribbenow, 66-70; Douglas Pike, *PAVN: People's Army of Vietnam* (Novato, CA: Da Capo Press, 1986), 45; Richard K. Dembrowski, *Eating Dinner with a Fork, Spoon, and Knife: How a corps executed MACV's One War Strategy* (master's thesis, School of Advanced Military Studies, 2009), 10.

This ability to mix regular and irregular forces was in line with our description of a hybrid threat, instead of a model of compound warfare with spatially distinct forces. COSVN had a specific charter to act as a holistic command for the effort in SVN, even if the NLF forces deliberately did not place themselves under a strict command-supported relationship. One useful way to view the operational relationship of the DRV's influence and regular forces to the NLF's influence and irregular forces is through metaphor: a father and son relationship where the father seeks long-term growth for his son, but maintains an ability to intervene with an assumed authority.[137] This was not a simple proposition of the VC's guerrilla forces supporting the NVA's main forces, as one would expect in a strictly compound warfare model. In some cases these roles reversed, with the NVA devolving into local forces.[138] Meanwhile, the VC could combine main force units, guerrillas, or local scouts as required, simultaneously acting as a reserve and support function for main force actions.[139] The effect of this mix was that Communist forces could support both forces simultaneously.[140] For example, captured enemy documents describe the melding of these forces in "three-front" attacks that closely coordinated local and main force units for the 1969 counter-offensive to reverse the losses of the previous year.[141]

Communist forces also employed a mixture of regular and irregular means in the fight, illustrated by Giap's claim that "[s]ophisticated [surface-to-air] missiles were used alongside primitive weapons."[142] This was especially prevalent in their adaptation of indirect firepower. In a period of six months, the NVA refined techniques to attack air bases and other fixed sites with improvised rocket attacks.[143] Even early in the American involvement, ARVN advisors noted the VC's judicious and accurate use of mortar systems designed to support infantry advances.[144] To manage the incorporation of modern weaponry in irregular units, COSVN integrated key technical experts into the NLF and VC, most of them returning back south after regroupment in 1954.[145] The mixing of regular and irregular means was not limited to offensive weaponry; it also pervaded service and support. COSVN's integration of training and sustainment operations enabled

[137] Military History Institute of Vietnam, *Victory in Vietnam: The Official History of the People's Army of Vietnam, 1954–1975* (Lawrence, KS: University of Kansas Press, 2002) trans Merle K. Pribbenow,76; Pike, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam*, 325-327.

[138] Military History Institute of Vietnam, 192, 248.

[139] Neil Sheehan, *A Bright Shining Lie: John Paul Vann and America in Vietnam* (New York: Random House, 1988), 206-211; Pike, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam*, 235.

[140] Dale Andrade, "Westmoreland was Right: Learning the Wrong Lessons From the Vietnam War," *Small Wars and Insurgencies* 19, no. 2 (June 2008): 146.

[141] Standing Committee of A26, "Matters to be Grasped when Performing the Ideological Task in the Party Body" in *Viet-Nam Documents and Research Notes, 'Decisive Victory: Step by Step, Bit by Bit'* (Lubbock, TX: Texas Tech University Vietnam Archive, 1969), 11.

[142] Vo Nguyen Giap, *How We Won the War* (Philadelphia, PA: RECON Publications, 1976), 13.

[143] Headquarters, United States Military Assistance Command-Vietnam, *PAVN Artillery (Rocket Units)-1967* (Saigon: United States Military Assistance Command-Vietnam, 1967), 1, 34.

[144] James B. Lincoln, "Letter to Clark Lincoln dated 14 August 1965 Comparing NLF and Saigon Forces." in *A Vietnam War Reader*, ed. Michael H. Hunt (Chapel Hill, NC: University of North Carolina Press, 2010), 66. Most veterans of America's contemporary counterinsurgencies also recognize the value of light, mobile indirect fires systems to an insurgent.

[145] Randall N. Briggs, "Compound Warfare in Vietnam" in *Compound Warfare: That Fatal Knot*, ed. Thomas M. Huber (Fort Leavenworth, KS: CGSC Press, 2002), 230.

larger conventional operations from safe havens in Cambodia and base areas within SVN itself. For the upcoming Binh Gia campaign in 1964, COSVN designated a specific headquarters section to develop a campaign plan. This plan utilized the irregular forces to prepare logistics and medical nodes for a massing regular force, and supported it with two regiments and an artillery group of main forces.[146]

Far beyond a mix of forces and means, the Communist forces active in SVN exhibited a mix of regular and irregular behavior. *Dau Tranh* theory provided the basis for this mixture. Giap described this effort to reach a decisive position through political and mobile warfare as "a form of fighting in which principles of regular warfare gradually appear and increasingly develop but still bear a guerrilla character."[147]

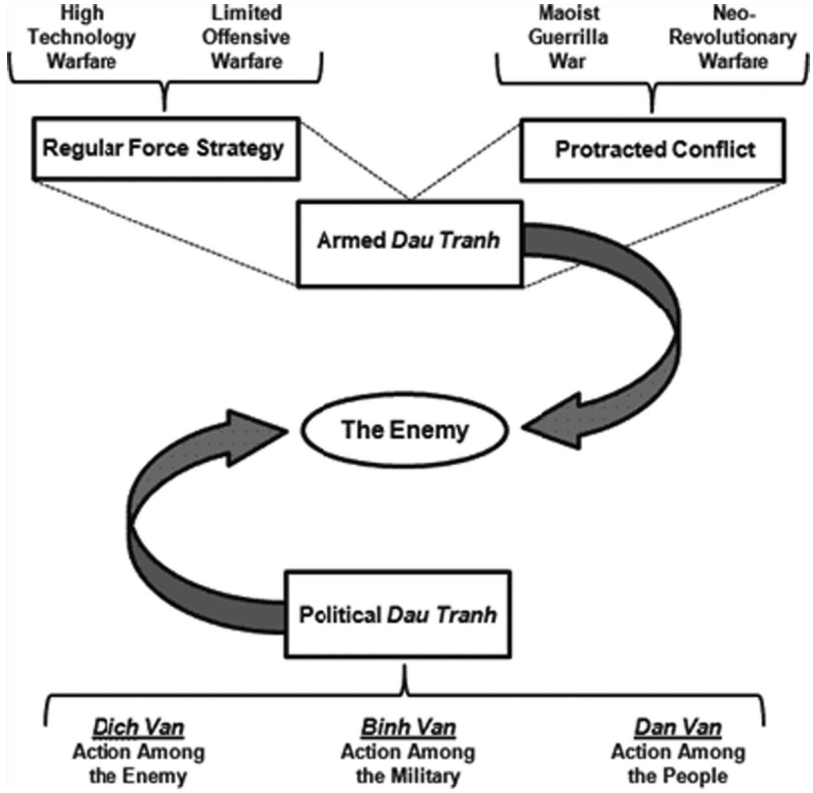


Figure 2. *Dau Tranh* Model[148]

[146] Military History Institute of Vietnam, 138-139.

[147] Vo Nguyen Giap, "The Resistance War Against French Imperialism" in *Guerrilla Warfare and Marxism*, ed. William J. Pomeroy (New York: International Publishers Company, 1968), 219.

[148] Pike, *PAVN: People's Army of Vietnam*, 212. This graphic is adapted from Pike's original work, to apply his graphical representation with the terminology and context herein.

Dau Tranh connotes an intense emotional struggle instead of a physical struggle, and consists of *dau tranh vu trang* (armed struggle) and *dau tranh chinh tri* (political struggle). This means that all actions taken in war are within the scope and framework of *dau tranh*; it is the complete blending of forms of warfare.[149] This achieved a requisite balance between civic action and military security. In practice, there was not an inherent distinction between the two struggles. Because the NLF formed to address 2,561 targeted villages instead of striving for a conventional capability like the *Viet Minh*, the VC village-level forces served as much of a psychological effect as they did a direct military value.[150]

Hybrid Warfare in Vietnam

Communist forces translated this dual effectiveness into positions of relative advantage across multiple domains. Although Leninist theory contended that armed propaganda and military strength should be inseparable and equal, information and influence activities took primacy in SVN.[151] Tellingly, even the regular forces of the NVA traced their military lineage to Giap's first *Viet Minh* armed propaganda team, which Ho Chi Minh saw as the "embryo of the National Liberation Army" in the struggle against the French.[152] The VC envisaged this communication of ideas and narratives as a seamless web, with dedicated cadres enabled by local security. In turn, these narratives symbiotically supported local security.[153] On a larger scale, Hanoi's narrative of an independent NLF helped to contest the war in the diplomatic domain, with the seemingly independent nature of the NLF proving to be "an enduring thorn in the side of Western anti-Communists."[154] Concurrently, the *Dich Van* program specifically targeted an American audience to convince them that victory was impossible, in order to constrain the use of American military capabilities such as air power.[155]

Communist forces melded these efforts in the military, political, and diplomatic domains in search of a synergistic effect.[156] But the synergistic effect of a hybrid threat was more evident in the employment of regular and irregular forces, means, and behaviors. Insurgents avoided large battles, and therefore took American units further away

[149] Ibid., 215-217.

[150] Pike, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam,* 109-111, 234-235.

[151] Hoang Ngoc Lung, *Indochina Monographs: Strategy and Tactics* (Washington, DC: U.S. Army Center for Military History, 1978), 122, 124.

[152] Ho Chi Minh, "Instruction to Establish the Vietnam Propaganda Unit for National Liberation" in *Guerrilla Warfare and Marxism*, ed. William J. Pomeroy (New York: International Publishers Company, 1968), 204; Pike, *PAVN: People's Army of Vietnam*, 28-29.

[153] Pike, *Viet Cong: The Organization and Techniques of the National Liberation Front of South Vietnam,* 124-132, 233, 237. For an illustration of this theory in practice, refer to: Propaganda and Training Section X69, *Study on the 1969 Spring—Summer Campaign SR6 COSVN* (Lubbock, TX: Texas Tech University Vietnam Archive, 1969).

[154] Van Canh Nguyen, *Vietnam Under Communism, 1975–1982* (Stanford, CA: Hoover Institute Press, 1983), 9; Briggs, 226 (quotation).

[155] Political Department, People's Liberation Army, *Outline of the Reorientation of Forthcoming Missions in 1970 For Elementary and Intermediate Cadre* (Lubbock, TX: Texas Tech University Vietnam Archive, 1970), 4, 10-11; Pike, *PAVN: People's Army of Vietnam*, 239-241.

[156] Standing Committee of A26, 5-6; Hoang, 125. General Hoang adds the economic, social, and cultural domains to his analysis of the threat.

from the population in an attempt to locate them. Exploited documents proved that both VC and NVA forces were trying to keep Army units fixated on non-decisive search-and-destroy operations away from the prized population centers on the coastal plains.[157] Meanwhile, Communist-liberated areas controlled by the NLF's People's Revolutionary Government acted as a base area for both regular and irregular forces. This *dan van* program of the larger *dau tranh* model added a noncontiguous base area for recruitment, sustainment, and protection, which was only nominally detectable by military means. GVN leaders attributed the most successful pacification efforts as 1969–1971, after the VC's failed Tet Offensive erased these base areas and decreased the resulting threat from Communist main force units.[158]

This synergistic effect supported the Communists' overall approach in SVN, that of exhausting the American and ARVN forces. Based on prior struggles against the Japanese and French, Giap viewed war as a long-term endeavor which sought to exhaust the enemy's manpower at its concentrated points while preserving the limited Communist manpower in SVN.[159] Even within the Maoist model of a three-phased war, localized conditions and enemy disposition meant that certain regions could be in different phases simultaneously to defeat the enemy where it was weakest.[160] The *dau tranh* model is deliberately protracted, with the assumption that eventually the incumbent force (in this case, both the GVN and its American support) is seen as accountable for contributing to this protraction.[161] This is evident in the VC slogan to promote ambush tactics, "fight a small action to achieve a great victory."[162] The effect of exhausting a larger force indirectly gained great traction, and by 1970 COSVN used the strain on American soldier morale as one of their three campaign objectives.[163]

The Operational Approach in Vietnam: A Strategy of Tactics

MACV's pursuit of a strategic aim in Indochina reflects the restrictive effect that social and political constraints manifest on an operational environment. America's grand policy tradition of containment easily translated into the narrower containment of Communist expansion in the contested areas of the Cold War.[164] As it appeared that communism was the next great expansionist threat after fascism, it naturally appealed

[157] Andrew F. Krepinevich, *The Army and Vietnam* (Baltimore, MD: Johns Hopkins University Press, 1986), 167, 192.

[158] Pike, *PAVN: People's Army of Vietnam*, 245; Tran Dinh Tho, *Indochina Monographs: Pacification* (Washington, DC: U.S. Army Center for Military History, 1978), 184.

[159] Giap, *Inside the Vietminh: Vo Nguyen Giap on Guerilla War*, I-3 to I-5, I-9 to I-10.

[160] Vo Nguyen Giap, *The Military Art of People's War* (New York Monthly Review Press, 1970) ed Russell Stetler, 179—181; Giap, *Inside the Vietminh: Vo Nguyen Giap on Guerilla War*, II-4, I-12. Although this localized focus may lead to some areas tending towards regular warfare before others, Giap still visualized an overall gradual buildup to mobile warfare with guerrilla characteristics.

[161] Pike, *PAVN: People's Army of Vietnam*, 219.

[162] Hoang, 126.

[163] Political Department, People's Liberation Army, 2.

[164] Walter McDougall, *Promised Land, Crusader State* (Boston, MA: Houghton Mifflin, 1997), 167, 190-193. McDougall's model of continuous policy traditions in American foreign relations does not cast "containment" as a radical departure from other traditions of orderly liberty, unilateralism, progressive imperialism, and expansionism. McDougall tenuously links another tradition of "global meliorism" to the strategic context of Vietnam, contending that the attempt to establish democracy in SVN took on the character of America's own domestic agenda. However, this monograph omits McDougall's global

to check its advance rather than seek its appeasement. This policy approach also had very pragmatic tones, since Truman contended that containment would cost roughly $400 million compared to the estimated $341 billion price tag for World War II.[165]

Containment of Communist expansion translated into the *Domino Theory* strategy of halting this expansion in Vietnam. This was not a stretch, since the Japanese expansion of World War II followed roughly the same axis of advance through China, Indochina, then to southeast Asia and beyond into the Pacific. As a theater strategy in Indochina, the basic objective remained the same through all presidential administrations: preventing a Communist takeover of SVN. Although the commitment of forces continued to increase in the 1960s, it remained a limited war. Since the bombing of military targets in the DRV itself was not a MACV activity, they considered efforts to destabilize and disrupt this strategic base area and infiltration route as a fundamentally separate action from attrition and pacification efforts within SVN.[166] Exacerbating this difficult strategic context was the unstable GVN, which impelled the political leadership to cultivate personal loyalties in ARVN, and thus an unstable military.[167]

The tactical actions in Vietnam took on a similarly disjointed characteristic, although it would be incorrect to assert that military security actions were completely divorced from the realities of pacification efforts. Unlike the *dau tranh* model though, they remained separate actions without a unifying logic. This reflected the Army's operational art doctrine at the time MACV was established:

> [t]he nature of the political situation at any time may require employment of armed forces in wars of limited objective. In such cases, the objective ordinarily will be the destruction of the aggressor forces and the restoration of the political territorial integrity of the friendly nation.[168]

The dissonance in this approach lies between the nature of "aggressor forces" since MACV visualized an idealized form of conventional warfare to maximize the Army's capabilities, and the nature of "restoration of the political territorial integrity" since the Diem regime was only marginally capable of effective governance. A focus on the destruction of an elusive enemy, coupled with a presumed dominance in conventional warfare, led Westmoreland to employ an approach of attrition. This is illustrated in the oft-cited discussion between an American and a NVA colonel during negotiations in 1975, in which the American colonel asserted that the NVA never defeated them on the

meliorism as a policy motivation, owing to the factual inaccuracies regarding the Strategic Hamlet program and a disjointed treatment of CORDS in *Promised Land, Crusader State*.

[165] McDougall, 163.

[166] Graham A. Cosmas, *U.S. Army in Vietnam: MACV, The Joint Command in the Years of Escalation 1962 to 1967* (Washington, DC: U.S. Army Center for Military History, 2006), 483.

[167] Hoang, 134; Harry G. Summers, *On Strategy: A Critical Analysis of the Vietnam War* (Novato, CA: Presidio Press, 1982), 87-89. In *On Strategy*, Harry Summers makes a compelling argument that the strategy itself was wrong, and that instead of countering insurgent forces in SVN the U.S. should have primarily oriented on military action against the DRV. However, this is a thin view of the historical strategic context at the outset of American commitment in 1954, since the recent experience in Korea created an overriding avoidance of Chinese or Soviet introduction to the conflict. It also discounts the fact that the NLF did not see itself as beholden to Hanoi, nor did it rely on the DRV for most of its resources.

[168] Headquarters, Department of the Army, *Field Manual 100-5* (Washington, DC: Department of the Army, 1954), 6.

battlefield. The NVA colonel pondered this, and presciently responded that this was true but irrelevant.[169]

Westmoreland contended that these large-scale search and destroy operations were erroneously portrayed in the media as a strategy instead of a tactic, which is a fair assessment.[170] However, he held the notion that rural areas did not hold intrinsic value except when the enemy was physically there, instead of understanding that their value lies in the ability to gird the population and resources thereby denying them to the VC.[171] Hence, the approaches of attrition and pacification were practically separate affairs for much of the war. MACV still saw pacification only as a corollary to military operations through 1967, and still discounted it in 1968 as a reason for VC village-level losses in rural areas. Intelligence analysts incorrectly attributed VC losses to the effectiveness of search-and-destroy operations, the internal displacement of over 2 million Vietnamese within SVN, and the VC's transition to main force operations.[172] Pacification was always a dominant element in policy but not in practice, evidenced by the low amount of American resources directly allocated in comparison to offensive military action.[173] Just prior to the NLF's Tet Offensive in January 1968, MACV established the Civil Operations and Revolutionary Development Support (CORDS) program to weight pacification efforts. Westmoreland and former presidential advisor Robert Komer melded the existing Office of Civil Operations and the MACV Revolutionary Support Directorate into one organization.[174] In the aftermath of extreme VC losses in the Tet Offensive, President Thieu initiated the Accelerated Pacification Campaign (APC) in order to exploit the opportunity afforded counterinsurgent forces. This was not a new concept, but an acceleration of resources guided by CORDS's contentious Hamlet Evaluation System.[175] The effect of the APC is that Communist forces began to rely on

[169] Summers, 1.

[170] William C. Westmoreland, "A Military War of Attrition" in *The Lessons of Vietnam*, ed. W. Scott Thompson and Donaldson Frizzell (New York: Crane, Russak and Company, 1977), 64.

[171] Westmoreland, *A Soldier Reports*, 150-151.

[172] Komer, 142; Headquarters, U.S. Military Assistance Command—Vietnam, *Viet Cong Loss of Population Control Evidence from Captured Documents* (Lubbock, TX: Texas Tech University Vietnam Archive,1968).

[173] Komer, 147.

[174] Richard Hunt, *Pacification: The American Struggle for Vietnam's Hearts and Minds* (Boulder, CO: Westview Press, 1995), 82, 87-92. Komer and General Creighton Abrams took positions as deputies for pacification and ARVN forces, respectively. Specifically, Westmoreland delegated command authority for pacification efforts to Komer, but as a civilian he was deliberately not a Deputy Commander. CORDS did not run through military unit chain-of-commands below Corps level, but instead via GVN administrative divisions down to the district level. This was an effort to prevent meddling by tactical military leaders as seen in Operation CEDAR FALLS. CORDS had civilian and military supervisor-subordinate roles and vice versa, to include ratings. It maintained the same six departments as the OCO (Refugees, Psychological Operations, New Life Development, Revolutionary Directorate Cadre, the *Cheu Hoi* program for Communist defectors, and Public Safety), plus four additional administrative departments (Management Support, Research and Analysis, Plans, and Reports and Evaluations).

[175] Eric Bergerud, *The Dynamics of Defeat: the Vietnam War in Hau Nghia Province* (Boulder, CO: Westview Press, 1991), 223; Vincent Davis, writing to John Paul Vann as cited in Sheehan, 697; Vietnam II Panel Discussion, U.S. Army Command and General Staff College Art of War Scholars Seminar, 18 January 2011, Fort Leavenworth, KS. The Hamlet Evaluation System attempted to quantitatively rate the qualitative indicators of pacification's progress at the lowest level. Military veterans of CORDS politely describe it as "tedious," or derisively as the "body count for pacification."

specific resources from the Ho Chi Minh Trail for the first time in the war, and the NLF ordered some VC forces to return to Phase I operations.[176]

One possible conduit to link the security line of operation and the pacification line of effort was through local security, the Territorial Forces.[177] Local security formed three rings: American and ARVN forces fighting Communists outside of populated centers, regular forces elements fighting smaller units to keep them from infiltrating towns and villages, and the police units countering Communist infiltration within the villages.[178] The handbook for American advisors stressed the advantages of a locally raised security force because they understood local political context, social conflicts, and terrain.[179] However, local security failed to unify the logic of attrition and pacification due to their lack of support, and the presence of an American unit remained the best correlation to security, as evidenced in the Tet Offensive.[180]

Ironically, *Vietnamization* was the only approach which effectively unified attrition and pacification.[181] On the heels of the APC and successful counter-offensive of 1969, President Lyndon B. Johnson deliberately countered Westmoreland's advice to launch a large-scale conventional counteroffensive, with Westmoreland claiming that Johnson "ignored the maxim that when the enemy is hurting, you don't diminish the pressure, you increase it."[182] The nuance that Westmoreland missed was that *Vietnamization* sought to increase pressure indirectly through an improved ARVN and pacification. General Creighton Abrams succeeded him as the MACV commander and described *Vietnamization* as three phases: the transition of ground combat to ARVN, increasing their capabilities for self-defense, and reducing American presence to assume a strictly

[176] Bergerud, 223, 224, 226, 234, 237, 246; Tran, 183; Ngo, 94; Summers, 96-97. The GVN and ARVN leadership saw the APC as the only effective way to meet the communist organizations head-on in accordance with American policies and goals. These measures were essentially coercive; only designed to provide a military presence in contested hamlets. CORDS viewed APC as the most successful GVN program to date, and VC-controlled hamlets dropped from 16.4% in January 1968 to 2.8% by December 1969. It also forced American and Vietnamese counterparts to align their effort, but American soldiers still exhibited distrust for ARVN. The APC also unwittingly masked the fact that the GVN was not stronger; the VC was just significantly weaker after the Tet Offensive. Thus, APC ensured that the real losers of the Tet Offensive was the VC, since it ensured the eventual victory would be dominated by cadres from the DRV.

[177] Vietnam Veteran, Interview BA030 by Aaron Kaufman and Dustin Mitchell, Fort Leavenworth, KS, 24 February 2011; Vietnam II Panel Discussion, U.S. Army Command and General Staff College Art of War Scholars Seminar, 18 January 2011, Fort Leavenworth, KS; Krepinevich, 173-175. Earlier attempts to establish effective local security forces included Combined Action Platoons (CAPs) and the Civilian Irregular Defense Group (CIDG). CAPs began as a test program in the I Corps area, utilizing Marine elements to live at the village level in an attempt to destroy VC support networks, protect the population, organize local intelligence nets, and train the Popular Force. Unfortunately, Marine leaders failed to arrange CAPs in critical areas akin to the 'oil spot' principle, and Army leaders successfully cast this as a do-nothing approach. CIDG elements, advised (and sometimes led by) American Special Forces advisors, operated in remote areas of operation in the central highlands to secure the population against VC infiltration. As such, they did not always have organic support capabilities and consequently served a limited, but successful role.

[178] Jesse Faugstad, "No Simple Solution," *Military Review* (July-August 2010): 34-35.

[179] Headquarters United States Military Assistance Command-Vietnam, *RF-PF Handbook for Advisors* (Saigon: United States Military Assistance Command-Vietnam, 1969), 6.

[180] Faugstad, 39, 41.

[181] Graham A. Cosmas, *U.S. Army in Vietnam: MACV, The Joint Command in the Years of Withdrawal 1968 to 1973* (Washington, DC: U.S. Army Center for Military History, 2006), 128-139. Although this was an attempt to arrange tactical actions, contemporary literature alternatively described it as the One War Strategy.

[182] Westmoreland, *A Soldier Reports*, 334.

advisory role.[183] For the first time, the effort in SVN oriented on protecting the population from Communist subversion rather than the destruction of the enemy force itself.[184] *Vietnamization* sought to serve as a unifying logic for all lines of effort in SVN, but it ultimately failed owing to poor execution and political constraints.[185] Some ARVN leaders recalled that the process actually looked more like the *Americanization* of ARVN since it integrated U.S. military equipment without an equal focus on doctrine, organization, or training to utilize it. When the American congress cut funding for ARVN advisory in response to the untenable political climate on the homefront, the psychological effect on the GVN and military leaders was even more deleterious than the material deficit.[186]

Analysis

Ultimately, these operational approaches failed to disrupt the Communists' logic of violence. In the strictest of interpretations, they were not operational approaches at all but rather attempts to achieve strategic success through a cumulative effect of tactical success. Certainly political constraints influenced this, but the chief failure was the inability of MACV to defeat armed *dau tranh* and political *dau tranh* simultaneously. Sir Robert Thompson wrote in 1969 that the focus in SVN should be on creating an intelligence structure to defeat the VC support network. This was an attempt to break the unifying logic of protracted *dau tranh* warfare, reflected in his assertion that "[i]n a People's Revolutionary War, if you are not winning you are losing, because the enemy can always sit out a stalemate without making concessions."[187] National Security Advisor Henry Kissinger added that "[t]he guerrilla wins if he does not lose. The conventional army loses if it does not win."[188] MACV fundamentally failed to disrupt this logic and actually bolstered it by pursuing a strategy of attrition. By engaging in disjointed search and destroy missions throughout the earlier phases of the war, the VC were never isolated from their base of support and simply had to survive to win.[189] MACV nominally disrupted the logic when the VC organization came unglued in the

[183] James Willbanks, *Abandoning Vietnam* (Lawrence, KS: University of Kansas Press, 2004), 21.

[184] Bergerud, 223, 241.

[185] Deputy Chief of Staff for Military Operations—U.S. Department of Defense, *A Program for the Pacification and Long-Term Development of South Vietnam, vol I* (Washington, DC: Department of Defense, 1966), 1-2; Komer, 142. *Vietnamization* was not the first initiative to unify these lines of effort. The March 1966 report "A Program for the Pacification and Long-Term Development of South Vietnam" (awkwardly abbreviated as PROVN) asserted that "Victory can only be achieved through bringing the individual Vietnamese, typically a rural peasant, to support willingly the Government of South Vietnam. The critical actions are those that occur at the village, district and provincial levels. This is where the war must be fought; this is where that war and the object which lies beyond it must be won." It offered six recommendations: Concentrate operations at the provincial level, give rural construction primacy among joint US-ARVN efforts, authorize direct involvement of U.S. officials in local GVN affairs, designate the U.S. ambassador as the sole manager of all U.S. activities, direct the sole manager to develop a single unified plan, and re-affirm to the world the strategic objective of a free and independent non-communist SVN. Ultimately, MACV suppressed the report but several of the themes were satisfied with CORDS.

[186] Hoang, 136; Willbanks, 285-286. Willbanks offers four conclusions on *Vietnamization*: it should have started earlier, earlier efforts should have focused on developing ARVN to counter the Communist subversion threat, later efforts towards a conventional ARVN should have focused on collective fire and maneuver skills instead of American technology and firepower, and the GVN should have addressed internal issues like corruption and poor leadership.

[187] Westmoreland, "A Military War of Attrition," 70; Briggs, 250.

[188] Henry Kissinger, "The Vietnam Negotiations." *Foreign Affairs* 47, no. 2 (January 1969): 214.

[189] Krepinevich, 170-171.

aftermath of the failed Tet Offensive, and the GVN consolidated these gains with the APC and RF improvements. Once these were in place, the NVA resorted to limited subversion to enable conventional campaigns in 1972 and 1975. This is perhaps the most ironic feature of the American experience in Vietnam; in that once the logic for violence was temporarily disrupted the enemy adapted a new logic which transitioned the conflict almost exclusively into regular warfare. The Communists no longer sought protraction, because they no longer needed American exhaustion.

The American effort also adopted an ill-suited uniform approach to hybrid warfare in SVN. The repetitive nature of search and destroy operations, harassment and interdiction fires, and aerial sorties seemed ideally suited to central statistical management.[190] This appetite for analysis led to a fruitless effort to create an independent variable for success in a complex environment. Secretary of Defense Robert McNamara employed over 100 social scientists in an attempt to quantitatively model SVN on a computer and simulate national-level behavior, once dismissing a qualitative assessment by saying "[w]here is your data? Give me something I can put into the computer. Don't give me your poetry."[191] This trend towards linearization and uniform solutions extended to MACV and ARVN leaders' understanding of the hybrid threat. They viewed the Communist threat as already in a Maoist Phase III when regular U.S. troops arrived in 1965, instead of considering the regional aspects of the threat as parts of a whole. Westmoreland's description of COSVN as a single unified command which directed the NLF also made it convenient to mirror image it as a conventional military headquarters.[192]

The overly linearized approach to separate attrition and pacification efforts is perhaps best understood through the metric of success, the body count. Aggregate Communist losses were carefully tabulated in an attempt to reach a conceptual *crossover point* at which attrition in SVN would exceed what the Communists could replace via the Ho Chi Minh Trail. However, this was an ill-framed concept since it assumed that increased forces and firepower would proportionately increase the body count, and that the VC and NVA were reliant on the DRV for resources. By 1966, VC requirements from outside of SVN were only 12 tons per day.[193] MACV refused to acknowledge these reports from national-level assets, along with journalist Bernard Fall's 1964 observation that the VC operation inside SVN was largely self-sufficient.[194] But after the Tet Offensive, MACV realized that warfare still had not reached a *crossover point* because the NVA (and the remaining VC) could control the tempo of fighting. Search and destroy operations

[190] Bousquet, 154.

[191] Ibid., 121.

[192] Westmoreland, "A Military War of Attrition," 62; *A Soldier Reports*, 55-57; Hoang, 4.

[193] Krepinevich, 168; Race, 198. All else was produced locally and infiltration from the north was negligible compared to locally-raised forces.

[194] Fall, *Street Without Joy*, 347; Van, 9-10; PAVN Officer, "Interview on the Intensified Military Effort, 1963—1964" in *A Vietnam War Reader*, ed. Michael H. Hunt (Chapel Hill, NC: University of North Carolina Press, 2010), 64-65. Other sources indicate a higher ratio of troops from the north, but still see a preponderance of recruitment from SVN. The debrief of a NVA officer in 1964 shows a clear pattern of replacing losses in liberated areas: '[e]ven if Hanoi stopped sending arms, supplies, and men to the Front, the Front would still be able to win because the Front responds to the aspirations of the people."

were an inefficient way to gain and maintain contact.[195] In this instance, the adaptive nature of the hybrid threat emerges; both COSVN and the NLF ironically realized that they could reach their strategic aim of exhausting the American military and public with steady attrition as they embarked on increased pacification operations.[196] While American units considered operational efficiency to be a mixture of gross eliminations and linear ratios of "exchange" and "contact success,"[197] a COSVN planning committee displayed a much better understanding of this aspect in hybrid warfare:

> While considering the situation, we should be flexible and avoid two erroneous inclinations. We should not adopt all principles too rigidly and neglect the evolution of the situation and the main, basic purposes of the Party; nor should we mix strategic policy with basic policy.[198]

Finally, the American effort failed to fuse tactical actions to strategic aims within the context that gave rise to a hybrid threat. This effort to amass quantitative data lacked any complimentary qualitative assessment to give it context, hence the actions this data prompted were in a fundamentally different frame of reference. By design, these systems were self-referential and therefore the context of social and political assemblages in SVN's village-level struggle was completely alien to MACV.[199] In appreciation of this, one American officer recalled that "[i]n sum, we were not able to break into another culture and into the communist organization."[200] Another break in context was rooted in the entire nature of warfare in Indochina. Communist leaders saw the revolutionary movement as a social progress with communal themes, while the GVN only saw it as a military process with nationalistic themes.[201] British advisor Sir Robert Thompson recognized in 1969 that adding resources to the GVN's military process instead of bolstering the governance and development progress was akin to "doubling the effort to square the error."[202] Arranging tactical actions only creates success when they can affect the adversary or their environment; independent search-and-destroy operations that are divorced from the context of a social and political struggle are the equivalent of re-arranging deck chairs on the *Titanic*.

---

[195] Carter Malkasian, *A History of Modern Wars of Attrition* (Westport, CT: Praeger, 2002), 192.

[196] Current Affairs Committee C69, *PLAF Assessment—Strategy* (Lubbock, TX: Texas Tech University Vietnam Archive, 1969), 36-38; Ninth COSVN Conference, "Resolution on a Shifting Strategy" in *A Vietnam War Reader*, ed. Michael H. Hunt (Chapel Hill, NC: University of North Carolina Press, 2010), 105; Briggs, 244. This metric also failed to account for the fact that the American people would not accept a ratio which equated the lives of their sons with the lives of the enemy.

[197] Headquarters, Department of the Army, *Sharpening the Combat Edge: The Use of Analysis to Reinforce Military Judgment* (Washington, DC: Department of the Army, 1974), 157-159.

[198] Standing Committee of A26, 3.

[199] Bousquet, 159.

[200] Headquarters, Department of the Army, *Sharpening the Combat Edge: The Use of Analysis to Reinforce Military Judgment*, 162.

[201] Race, 141, 179-180.

[202] Thompson, *No Exit From Vietnam*, 165. Apparently, Thompson recognized that complexity and non-summative properties work both ways.

Conclusion

The preceding analysis should not paint a picture of doom and gloom over the canvas of hybrid warfare in SVN. By 1970, the combined forces of MACV and ARVN stood at a position of relative advantage, enabled by both the near-complete destruction of the VC as a viable force and a strengthened GVN. However, this was also when COSVN realized that the protracted conflict could still prevent the Americans from achieving termination criteria at a position of political advantage via a military advantage in SVN.[203] The NVA developed more regular warfare capacity for a conventional invasion, and increasingly used their irregular forces, means, and behaviors to enable this capability.[204]

The American military spent the post-Vietnam years institutionally wary of irregular warfare and counterinsurgency. If a theorist postulated the concept of hybrid warfare in the aftermath of the Vietnam War, the Army may have institutionally avoided it as well. Then Iraq happened. As in SVN, they would spend years adapting and spending untold blood and treasure to fight a hybrid threat. This threat was like no other, and it required an operational approach like no other. However, in Iraq the Army would harness a more organizationally mature understanding of operational art, enabling this pathway to termination criteria at a position of advantage. In short, the Army would learn to charge the toreador instead of the bull.

5. Operation Iraqi Freedom: The School of Piranhas

> We're not playing together. But then again, we're not playing against each other either. It's like the Nature Channel. You don't see piranhas eating each other, do you?—Rounders, 1998

Much in the way history views World War II as conventional warfare, it views OIF as irregular warfare. Since this monograph considers hybrid warfare on a continuum instead of a distinct form of warfare in a series of discrete menu choices, the study of OIF through the lens of hybrid warfare may assist Hoffman's metaphoric attempt to break the pristine bins of Western categorization. Fundamentally, Iraq is one of those large gray spaces in between existing models. The model of an insurgency-counterinsurgency dynamic looks to be the correct framework for analysis at first blush, but this largely owes to the influence of the counterinsurgency doctrine which informed the ultimate operational approach. As such, it is bound to shape the way we view it in early attempts of qualitative historical analysis. However, it is fundamentally insufficient to separate the ground war of 2003 and the following stages of insurgency, terrorism, and communal conflict in Iraq. Likewise, it is insufficient to completely dismiss the episodic examples of regular warfare, no matter how infrequent they were. They

[203] Political Department, People's Liberation Army, 16.

[204] Lewis Sorley, *Vietnam Chronicles: The Abrams Tapes 1968–1972* (Lubbock, TX: Texas Tech University Press, 2004), 376; Andrade, 147. Andrade refutes Krepinevich's argument in *The Army and Vietnam* that a secured countryside would have withstood the NVA's 1973 and 1975 campaigns; he illustrates that continued pacification would not have addressed "the enemy lurking in the shadows" (across the border) to sweep away these gains. This reflects Abrams' earlier contention that "[y]ou just can't conduct pacification in the face of an NVA division" no matter the standoff.

are all profoundly interconnected. In contrast to a model of hybrid threat organization such as COSVN, the elements of the hybrid threat in Iraq were only harmonized by a common aim. In this way, the American Army in OIF faced a threat akin to the school of piranhas.

The Context of Conflict in Iraq

Modern Iraq sits astride the fault lines between religiously distinct Shi'a and Sunni Muslims, as well as ethnically distinct Arab, Persian, and Kurdish populations.[205] At roughly 437,000 square kilometers, it is slightly larger than the state of California. The landscape is generally a vast desert, interrupted by fertile river valleys and rocky escarpments.[206] Demographically, the pre-war population of 24.6 million was roughly 60 percent Shi'a and 35 percent Sunni, with traces of Christian and other religious communities. Ethnically, the Arab population stood at an 80 percent majority, with a Kurdish minority of 15 percent and socially isolated communities of Turkomen, Assyrians, and other groups.[207] Consequently, most initial operational approaches were couched in terms of Shi'a and Sunni or Arab and Kurd models.[208]

American intervention in Iraq began in 1990 with Operation Desert Shield, followed by the ground invasion of Iraq in 1991.[209] After a decade of patrolling no-fly zones to protect Kurdish and Shi'a populations, U.S. Deputy Secretary of Defense Paul Wolfowitz made a case for a pre-emptive regime change in Iraq almost immediately after the al-Qaeda's terrorist attacks against the United States in 2001.[210] The U.S. secured a nominal international backing from the United Nations and formed a coalition of limited

[205] Johnson, *The Biggest Stick: The Employment of Artillery Units in Counterinsurgency*, 164-262. This section on *Context* draws heavily on the author's original work while researching the employment of artillery units in counterinsurgency operations. It is intended as a brief overview of the cultural, historical and strategic context, not an exhaustive treatment on the roots of conflict in Iraq.

[206] 1st Infantry Division, *Soldier's Handbook to Iraq* (Wurzburg, GE: 1st Infantry Division, 2004), v. 1st Infantry Division issued this handbook to soldiers before deployments to Iraq in 2004. It is representative of handbooks developed internally by U.S. Army units in the earlier years of the war. These handbooks are thick with background facts of Iraq and useful Arabic phrases, but neglect a thorough analysis of culture in Iraq.

[207] 1st Infantry Division, v.; Charles Tripp, *A History of Iraq* (New York: Cambridge University Press, 2005), 8-9. Equally important is the demographic aspect of Iraqi society in terms of urban and rural populations. Iraq has many large and modern metropolitan centers, to include Baghdad at over 5.6 million residents, Mosul (in the north) and Basra (in the south) each have over 1 million inhabitants. Kurdish population centers in northern Iraq include Irbil (839,600), Kirkuk (728,800), and As Sulaymaniyah (643,200); predominately Shi'a Arab cities to the south include An Najaf (563,000), Karbala (549,700), and An Nasiriyah (535,100). Cities in the Sunni Arab heartland are considerably smaller: Fallujah and Ramadi in the Euphrates River Valley, and Balad, Samarra, Tikrit, and Bayji in Tigris River Valley.

[208] Interview BF020, Civilian Advisor to MNF-I, Interview by Richard Johnson and Aaron Kaufman, Boston, MA, 11 March 2011. Disaffected Shi'a exiles and nationalistic Kurds that influenced early U.S. plans for civil re-development in Iraq drove this perception among strategists and planners. Arguably, urban Sunni and Shi'a nationalists had more in common than urban and rural Islamists from the same sect or ethnicity in 2003.

[209] Thomas E. Ricks, *Fiasco* (London: Penguin Press, 2007), 5-6. Critically, the Coalition force failed to destroy the core of the 80,000-strong Republican Guard during this campaign before terminating operations at a position of military advantage.

[210] Ricks, *Fiasco*, 13-15.

partners, eventually leading a multi-divisional ground offensive in March 2003.[211] Coalition forces took measures to avoid a perception of occupation, but they were the only form of security allowed in most areas immediately after the ground campaign culminated in the collapse of Saddam Hussein's Ba'athist regime.[212]

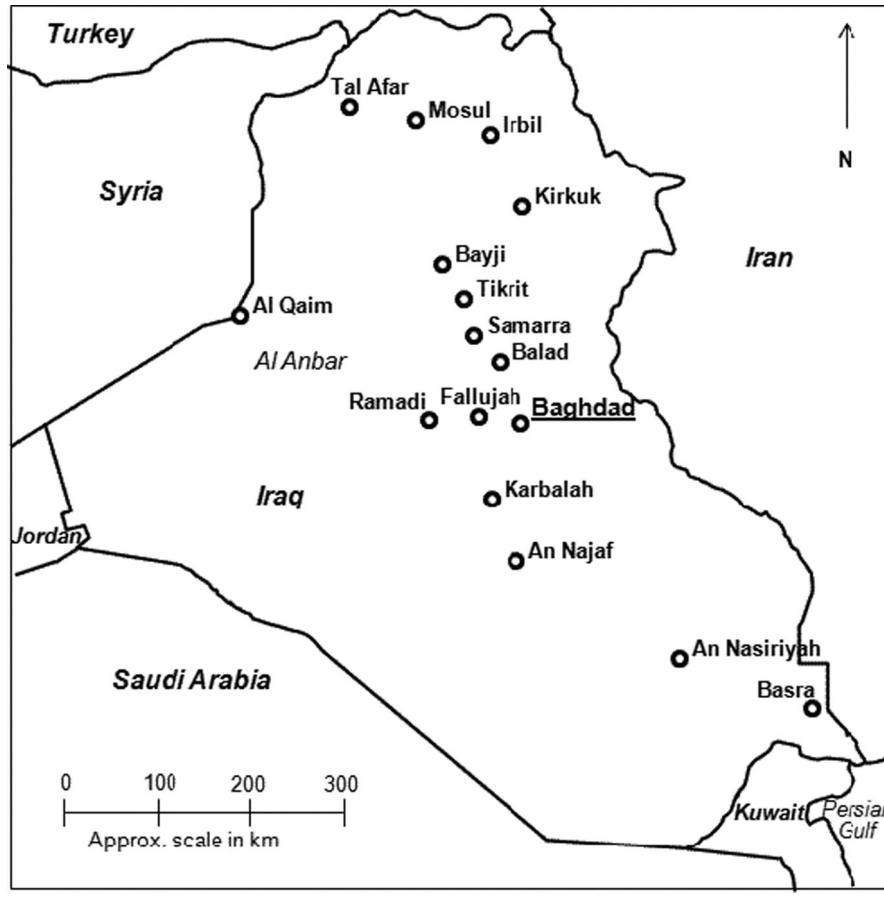


Figure 3. Iraq, 2003

The Hybrid Threat in Iraq: Passive Interconnection

The complex organization of the hybrid threat in Iraq belied the Army's attempt to organize against a single yet amorphous enemy. As attacks rose dramatically during the

[211] Michael R. Gordon and Bernard Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon Books, 2006).This is merely a summary of "The Ground War," which will be examined later as the first phase of hybrid warfare. One of the best sources for further research into this conventional campaign is Gordon and Trainor's comprehensive account and analysis.

[212] These measures included the prohibition from flying American flags or displaying any other overt signs of foreign power within direct view of the Iraqi population.

summer of 2003, many analysts saw the threat in terms of a more cohesive quilt, but several commanders began to understand the patchwork nature: "we are fighting former regime-backed paramilitary groups, Iranian-based opposition, organized criminals and street thugs."[213] These formerly "mutually antagonistic" elements did not work together directly, except for in isolated instances. At least nine disparate organized groups concurrently emerged, and additional elements of tribal protection and criminality created a *passively* interconnected threat array.[214] RAND Corporation analysts John Mackinlay and Alison Al-Baddawy characterized this as a Federated Insurgency Complex, "the focal point of several different strands of violent energy…the product of different local, national, and international communities and subversive organizations."[215] The hybrid threat in Iraq was also adaptive, using its initial advantage in local perception and resources to develop lethal capabilities against militarily superior forces. This was particularly evident in Baghdad, where Shi'a-based groups adopted explosively formed projectiles and sniper attacks against American forces.[216] Throughout the war, groups adapted punctuated lethal attacks that led to an American focus on individual force protection, making soldiers appear as "storm troopers" and vehicles appear as "urban submarines" while on patrol.[217] This effectively isolated the soldiers from the local population, once again giving the threat an advantage in their ability to penetrate the population.

Mixing regular and irregular means was also prevalent in Iraq, a further indicator of the adaptive nature of the threat. After the rapid advance of the initial land campaign by coalition forces, weapons were plentiful at many abandoned Iraqi Army bases. As some units approached, they discovered instances such as the one in Tikrit wherein a unit discovered 30 Iraqis openly looting weapons.[218] In a 2009 interview, one sheikh from Ramadi casually mentioned gaining 80 rocket propelled grenades and additional light machine guns from an unsecured base after meeting the coalition forces and telling them about it the day before.[219] The availability of small arms, indirect fires weapons and high explosives was another key ingredient in this Petri dish for a hybrid threat: the enemy was bound only by its imagination to innovate complicated devices for coordinated attacks.

The hybrid threat in Iraq displayed a modicum of regular forces, but it was episodic at best. This may be the primary reason for a hesitation to view the "school of piranhas" as a hybrid threat, in that it nearly fails one of the most visible tests. However, this viewpoint predicates upon the Western martial tradition's concept of regular and irregular

[213] Peter R. Mansoor, *Baghdad at Sunrise: A Brigade Commander's War in Iraq* (New Haven, CT: Yale University Press, 2008), 356. At the time of this observation (June 2003), Colonel Mansoor was a brigade commander in eastern Baghdad.

[214] Ahmed S. Hashim, "The Insurgency in Iraq," *Small Wars and Insurgencies* 14, no. 3 (August 2003): 5-9. The notion of a "passive" interconnectedness is the author's own characterization.

[215] John Mackinlay and Alison Al-Baddawy, *Rethinking Counterinsurgency* (Santa Monica, CA: RAND, 2008), 58.

[216] Ricks, *The Gamble,* 172. Ricks cites the example of C/2-16 IN in Adamiyah.

[217] David Kilcullen, *The Accidental Guerrilla* (Oxford, UK: Oxford University Press, 2009), 137. At the time of his observations, Kilcullen was working as a counterinsurgency advisor to Petraeus.

[218] Gordon and Trainor, 447.

[219] Timothy S. McWilliams, *Al-Anbar Awakening: U.S. Marines and Counterinsurgency in Iraq, 2004–2009* (Quantico, VA: Marine Corps University Press, 2009), 86.

forces, not upon an Eastern concept.[220] As such, the difference between regular and irregular forces' interactions in Iraq as compared to Vietnam or Lebanon is really a difference in degree, not a difference in kind. Although they never organized in hierarchical elements like VC main forces, disaffected professional military personnel acted in small but lethal ambushes, especially in Sunni strongholds close to former army bases such as Ramadi and Tikrit.[221] With smaller elements conducting similar tactics, it is harder to distinguish between regular and irregular forces unless one focuses on artificial externalities such as uniforms. Even so, regular and irregular forces worked synergistically as an aspect of warfare in Iraq during the initial campaign,[222] and in response to isolated clearing operations such as the ones in Fallujah.[223] But the question remains: why was there a tangible mix of hybrid means and behaviors, but only fleeting instances of hybrid forces? Most likely, it was because the initial campaign and overt clearance operations were the few times the threat had significant base areas and an opportunity to formalize the regular components' relationships. Since the mix of regular and irregular forces is the most visible indicator of a hybrid threat, this is the primary reason most analyses overlook it and view the conflict through the lens of an insurgency-counterinsurgency dynamic.

Hybrid Warfare in Iraq: Applying Kilcullen's Venn Diagram

This insurgency-counterinsurgency dynamic only addresses a portion of warfare in Iraq, albeit the vast majority.[224] However, it is fundamentally insufficient to explain the whole of the system with only a descriptive snapshot of a given space or time in the conflict. It is also an artificial distinction to separate aspects of warfare, and it is prone to errors if the cognitive boundaries are drawn incorrectly. Much in the same way an enemy can exploit physical unit boundaries when they are incorrectly overlaid on a high-speed avenue of approach, the adroit enemy can also exploit the seams between

[220] Patrick Porter, *Military Orientalism: Eastern War Through Western Eyes* (New York: Columbia University Press, 2009), 172, 179. This is strikingly similar to the IDF's generalized preconception of an Arab enemy that pervaded the 2006 conflict in Lebanon, ignoring the fact that while Arab armies are historically less successful in regular campaigns, they have a decent record in irregular campaigns.

[221] Ahmed S. Hashim, *Insurgency and Counterinsurgency in Iraq* (Ithaca, NY: Cornell University Press, 2006), 33.

[222] Ibid., 12-16. The Hussein regime conceptually understood the value in an admixture of regular and irregular units, but did not implement them to sufficiently exhaust U.S. forces indirectly. In spite of over 4,000 foreign fighters to complement the *Saddam Fedayeen*, they failed to stop (or even significantly delay) the approach to Baghdad.

[223] Carter Malkasian, "Counterinsurgency in Iraq: May 2003–January 2010," in *Counterinsurgency in Modern Warfare*, ed. Daniel Marston and Carter Malkasian (Oxford, UK: Osprey Publishing, 2010), 290-291, 296; Matt M. Matthews, *Operation Al Fajr: A Study in Army and Marine Corps Joint Operations* (Fort Leavenworth, KS: Combat Studies Institute Press, 2006), 37, 45-46; Combat Studies Institute, *Eyewitness to War: The US Army in Operation Al Fajr, An Oral History* (Fort Leavenworth, KS: Combat Studies Institute Press, 2006). The two battles of Fallujah (March–April 2004 and November–December 2004) included complex obstacle systems covered by fires, strongpoint defenses of 40 -50 fighters, and well-constructed fighting positions much like a contemporary U.S. Army or Marine unit would defend urban terrain. For first-hand accounts of the regular warfare aspects of this engagement, see *Operation Al Fajr* and *Eyewitness to War.*

[224] Hashim, *Insurgency and Counterinsurgency in Iraq*, xviii; Headquarters, Department of the Army, *Field Manual 3-24: Counterinsurgency* (Washington, DC: Department of the Army, 2006), p. 3-14. Hashim points out that the insurgency began during a perceived foreign occupation, before the constitution of a legitimate host nation government. Interestingly, according to U.S. Army counterinsurgency doctrine (developed specifically to address doctrinal shortcomings highlighted in OIF) this would categorize it as a "resistance movement" which would "tend to unite insurgents with different objectives and motivations."

forms of conflict if a force task-organizes to fight them separately.[225] Additionally, it only addresses a certain set of population grievances which led to hybrid warfare, not the underlying reasons for protracted conflict.

David Kilcullen's explanatory model for warfare in Iraq provides this critical insight, highlighting its nature as warfare across multiple domains of conflict. Insurgency, terrorism, and communal conflict formed the major domains of conflict created by the underlying dysfunction of collapsed national systems in need of rebuilding.[226]

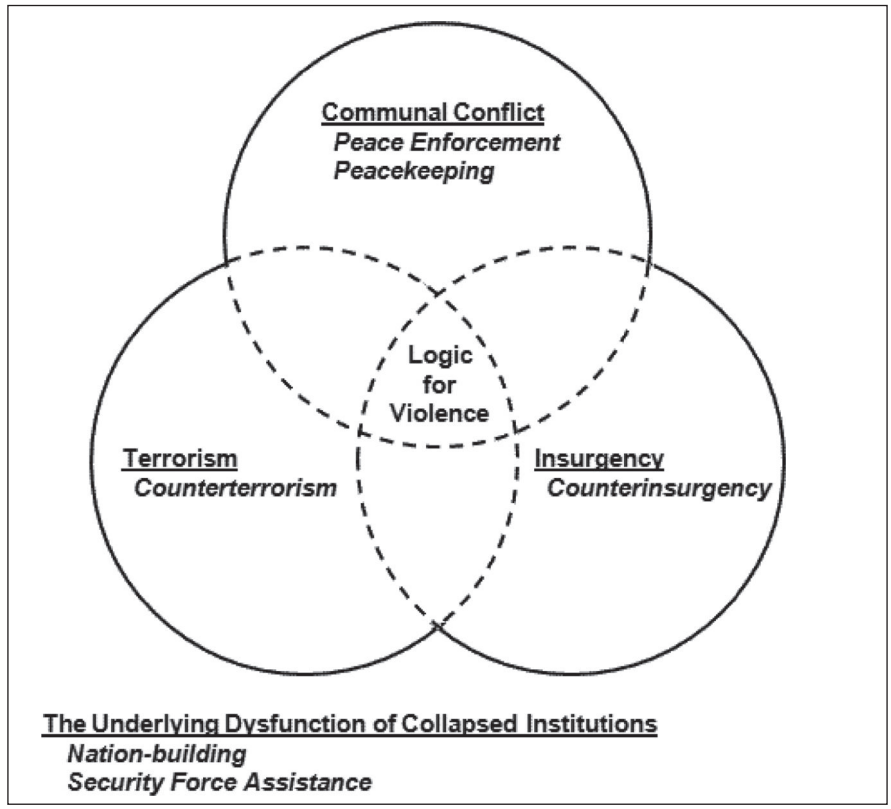


Figure 4. A Model of Hybrid Warfare in Iraq[227]

Kilcullen proposes in *The Accidental Guerrilla*:

> Iraq, then, is not a pure insurgency problem but a hybrid war involving what we might call "counterinsurgency plus." …Effective counterinsurgency is a sine qua non for success, but it is still only one component within a truly hybrid conflict.[228]

[225] Hoffman, "The Hybrid Character of Modern Conflict," 46. As Hoffman observes: "It is not clear how we adapt our campaign planning…in Iraq we continue to separate warfighting from "population-centric counterinsurgency," or think of counterterrorism and counterinsurgency as two separate approaches."

[226] Kilcullen, *The Accidental Guerrilla*, 148-151.

[227] Ibid., 150. This graphic is adapted from Kilcullen's original work, to apply his graphical representation with the terminology and context herein.

[228] Ibid., 152.

Although population-centric counterinsurgency approaches proved successful, they were not enough to deal with the broader issues. As a complex and constantly changing set of problems, interconnected forms of warfare amplified conflict in Iraq. An action to address a problem in one domain exacerbated conflict in another, often times unpredictably. As such, any analysis of OIF must bear in mind that there was not a definitive *enemy* in the traditional sense, since various groups alternately considered each other as enemies or partners based on the ecology of the conflict. Relative to coalition forces, it is somewhat more accurate to view the disparate insurgent or sectarian groups as *rivals*, each with their own brand of security and governance as the goal.

The clearest example of this is counterinsurgency actions intensifying communal conflict. Even in applying nuanced local solutions, they were framed in the aforementioned Sunni-Shi'a or Arab-Kurd model and subsequently fanned the flames of sectarian violence that was relatively unheard of in Iraq's recent past. As one senior political advisor to Multi-National Force—Iraq (MNF-I) described it, "[y]ou don't have a history of large inter-communal violence. If you go into any society and collapse its institutions, what is the outcome?"[229] Terrorism exploited opportunities in this setting, with al-Qaeda and Quds force activities seeking to further their transnational extremist goals. Supra-domain combinations arose as well, enabled by the trend of increasing global Muslim awareness from Niger to The Philippines arising from new access to the internet and dedicated satellite media such as *Al-Arrabiya* and *Al-Jazeera*.[230]

This was the synergistic effect which faced coalition forces as warfare increased in intensity from 2003 to 2007. Distinct from the deliberate aims of *dau tranh* in Vietnam, this was an inadvertent consequence of the school of piranhas. The sum effect of warfare in Iraq was considerably more than the constituent parts. This initially led to many commanders' frustrations as to why an army, which swiftly defeated a large conventional force, could not contend with a handful of insurgents. This was evidenced in the fact that early attempts to introduce a purely military or purely political solution in one problem set masked or negated gains in another problem set, reinforcing the notion that "[w]hile 'war amongst the people is political,' it is still a kind of war."[231] The experience of one unit's attempt to mentor paramilitary forces and put an Iraqi face on operations in 2004 provides an illustration of the non-summative results in a profoundly interconnected environment:

> The national police commandos that they brought up were very aggressive—we didn't know it at the time, but the guys that were being brought in were getting after the Sunni population in Samarra and we thought it was great—but it really was the beginning of the sectarian violence. We didn't recognize it at the time, but it was just an opportunity to whack Sunnis and they didn't care if they were insurgents, terrorist or otherwise.[232]

[229] BF020, Interview.

[230] Mackinlay and Al-Baddawy, 39-42.

[231] Brian Burton and John Nagl, "Learning as We Go: the U.S. Army Adapts to COIN in Iraq, July 2004–December 2006," *Small Wars and Insurgencies* 19, no. 3 (September 2008): 323.

[232] BD010, Field Grade Officer, Interview by Benjamin Boardman and Dustin Mitchell, Fort Knox, KY, 14 March 2011. The respondent had direct knowledge of Operation Baton Rouge, a combined operation to clear insurgent and terrorist forces in Samarra.

Although the synergy of hybrid warfare was not a purposeful effort since it relied on the harmonization of disparate elements, the effort to protract warfare in order to exhaust American forces was a deliberate aim by all. With respect to coalition military forces in Iraq, rivals sought to make warfare so untenable and uneconomical that the psychological strain would be too much to bear in an American cost-benefit calculation.[233] Insurgents posited that they could outlast the coalition via slow attrition from continued attacks, since they perceived this was just another chapter to a long struggle in which coalition forces lacked resolve.[234] In the realm of communal violence, Shi'a groups in Baghdad tried to weaken the vulnerable Sunni population by mixing lethal extra-judicial killings and legitimate government actions. One Brigade Combat Team commander recalled that by these means, "[t]hey were trying to get the Sunnis to quit through a campaign of exhaustion."[235] Sunni Arab groups such as al-Qaeda in Iraq employed the same logic, economically starving Shi'a and Turkomen communities in the north to complement targeted killings, in a broad attempt to exhaust and realign the population.[236] With respect to the American homefront, rivals sought to increase casualties in Iraq "to the point of making the authority in charge of the occupation guilty before its own citizens."[237] Ironically, the growing gap between the American public and the all-volunteer military made this much less likely than in Vietnam.[238]

The Operational Approach in OIF: Resolve and Opportunity

Another benefit of this all-volunteer force is that many of the same commanders and planners would return to Iraq repeatedly during OIF. This directly enabled the adaptation of improved understanding and context, a collective intuition that in turn created refined tactics and approaches to the complex environment. While this study strives to avoid a narrative of early villains yielding to later heroes in OIF, the marked improvements over time are undeniable.

As with the Vietnam War, strategic context framed operations and the characteristics of hybrid warfare. In the incipient phases of the Global War on Terror, President George W. Bush augmented the grand policy traditions of containment through deterrence with the option of pre-emption.[239] In this manner, the initial charter for OIF was running

[233] Hashim, *Insurgency and Counterinsurgency in Iraq,* 178-179.

[234] Carter Malkasian, "The Role of Perceptions and Political reform in Counterinsurgency: The Case of Western Iraq, 2004–2005," *Small Wars and Insurgencies* 17, no 3 (September 2006): 379-385. Malkasian describes four events that reinforced this notion within Sunni groups (the April 2004 uprisings, the ceasefire in Operation Al Fajr I, the June 2004 transfer of sovereignty, and continued promises of a timetable-based U.S. withdrawal), and five events that reversed the notion (suppressing JAM in Najaf, Operation Al Fajr II, partnered presence for security, successful national elections, and the adoption of a conditions-based withdrawal).

[235] BH020, Field Grade Officer, Interview by Mark Battjes, Ben Boardman, Robert Green, Richard Johnson, Aaron Kaufman, Dustin Mitchell, Nathan Springer, and Thomas Walton, Washington, DC, 21 March 2011.

[236] BH070, Iraqi Mayor, Interview by Mark Battjes and Robert Green, Washington, DC, 25 March 2011. This mayor had direct knowledge of these efforts in Tal Afar.

[237] Hashim, *Insurgency and Counterinsurgency in Iraq*, 179.

[238] BF010, Former Army Officer, Interview by Richard Johnson and Aaron Kaufman, Boston, MA, 11 March 2011.

[239] John Lewis Gaddis, *Surprise, Security, and the American Experience* (Cambridge, MA: Harvard University Press, 2004), 86; BF010, Former Army Officer, Interview by Richard Johnson and Aaron Kaufman, Boston, MA, 11 March 2011. This strategic analyst (with experience as an Army officer) provided the following

out politically, prompting the Baker-Hamilton Commission's report to Congress in the summer of 2006.

Until then, General George Casey's Transition Bridging Strategy personified the operational approach.[240] This approach used the logic of transitioning Iraqi security responsibility and provincial control as capabilities matured. As such, coalition forces would retreat to larger forward operating bases (FOBs). Many commanders expressed this with the phrase "as we stand down, they stand up."[241] Consequently, Casey directed the establishment of *transition* as a separate line of effort rather than as a unifying logic, against the advice of some of his staff.[242] With tactical units stressed to leave urban areas for remote FOBs, there was not an adequate provision for those units who did not have a competent Iraqi counterpart yet.[243] One officer remarked that this was a flawed operational construct, in that "[w]e were always six months from leaving Iraq."[244] Communal violence and terrorist actions rose considerably in 2006, with killings peaking at about 125 per night in the *amanat* of Baghdad alone.[245] Even in the face of such contradictions, Casey's command and U.S. Central Command (CENTCOM) continued to focus on operational disengagement via transition. One strategic plans officer recalls:

> In 2006, after I went and spent time with [3rd Armored Calvary Regiment], I was on General Abizaid's staff. The CENTCOM planning assumption was that we were in a lockstep march from 20 to 10 Brigades by 2006. I don't know if you remember but [2nd Brigade, 1st Armored Division] wound up being off-ramped and went to Kuwait, and [2nd Brigade, 1st Infantry Division] came in behind them. When things were at their worst in Iraq in 2006, the CENTCOM commander was off-ramping brigades.[246]

---

insight in 2011: "The purpose of the GWOT when it began, to my mind, was informed by a conviction, an honestly held conviction by people in the Bush administration, that the only way to really guarantee there wouldn't be another 9/11 was to fix the dysfunction of the Islamic World; to transform the Islamic World, and therefore remove those conditions giving rise to *jihadism*."

[240] Ricardo Sanchez, *Wiser in Battle: A Soldier's Story* (New York: HarperCollins, 2008), 444-446; Burton and Nagl, 304, 306; Ricks, *Fiasco*, 173; George Packer, "The Lesson of Tal Afar," *The New Yorker* 82, no. 8 (10 April, 2006), www.newyorker.com/archive/2006/04/10/ 060410fa_fact2 (accessed 13 May 2011); Peter Chiarelli and Patrick Michaelis, "The Requirements for Full-Spectrum Operations," *Military Review* 85, no. 4 (July–August 2005): 4. Through 2004, there was effectively no operational approach in Iraq. There was no link between the civil reconstruction effort at the Coalition Provisional Authority and the military headquarters, CJTF-7. Lieutenant General Ricardo Sanchez did not have a published campaign plan during his command, nor did he provide the capacity to guide unified action. Sanchez claims that CENTCOM did not enact a plan for reconstruction in Iraq, and that he was initially unaware the plan even existed. Given this, and the fact that Army units still held a conventional mindset to win large-scale maneuver wars, many general officers doubt any commander could have done well.

[241] BA010, Brigade Commander, Interview by Richard Johnson and Thomas Walton, Fort Leavenworth, KS, 22 February 2011.

[242] BI020, Battle Group Commander, Interview by Aaron Kaufman and Thomas Walton, United Kingdom, 31 March 2011. The respondent augmented the MNF-I staff at the time.

[243] BA010, Brigade Commander, Interview by Richard Johnson and Thomas Walton, Fort Leavenworth, KS, 22 February 2011.

[244] BH030, Iraq Veterans Panel, Interview by Mark Battjes, Robert Green, Aaron Kaufman, and Dustin Mitchell, Washington, DC, 22 March 2011.

[245] Kilcullen, *The Accidental Guerrilla*, 124, 126.

[246] BH030, Interview. The units that this respondent refers to are: the 3rd Armored Cavalry Regiment, the 2nd BCT of the 1st Armored Division, and the 2nd BCT of the 1st Infantry Division, respectively.

Within risk lies opportunity, even if it is thickly veiled. Unlike the Vietnam War, the strategic context in 2006 would avail just such an opportunity, but it required American forces to fundamentally reframe the operational approach. The Baker-Hamilton report advocated a conditions-based withdrawal relying on milestones for Iraqi national reconciliation, security and governance.[247] In response, the neoconservative American Enterprise Institute (AEI) developed a competing option for continued operations in Iraq, opening with the premise that "[v]ictory is still an option in Iraq."[248] Dr. Frederick Kagan led the AEI effort to develop an alternative to the findings in the Baker-Hamilton Commission's report, which benefitted from both the official and unofficial involvement of military officers with experience in Tal Afar. Additionally, Kagan leveraged a personal relationship with retired General Jack Keane, who also mentored then-General David Petraeus and then-Lieutenant General Raymond Odierno.[249] In striking detail, the group visualized Baghdad as the decisive effort in Iraq with an operational approach which required: balancing improved Iraqi Security Forces with protecting the population, clearing Sunni and mixed-sect neighborhoods, maintaining security to reconstitute governance and services, supporting the Iraqi central government's ability to exercise power, and a surge of seven army brigades to support this expanded approach.[250]

Simultaneously, Odierno arrived in Iraq to take command of Multi-National Corps—Iraq (MNC-I). Within the first 60 days, he halted the effort to retreat to the large remote FOBs, in clear opposition to Casey's Transition Bridging Strategy. Significantly, Odierno operationalized AEI's approach by adding a focus on securing Shi'a neighborhoods against Sunni al-Qaeda in Iraq-affiliated networks, and placing an equal emphasis on the Baghdad belts.[251] In this, Odierno provided the first elucidation of an operational approach to the complex warfare in Iraq, colloquially known as *The Surge*:

> [Odierno] and Colonel Jim Hickey figured out that it was all about locating the enemy's safe havens and sanctuaries and disrupting those . . . that's what the battle of the belts was all about. I don't think anyone had that concept. Although I think Colonel McMaster had an appropriate solution, it was not applied on a broad

[247] Baker-Hamilton Commission, *Iraq Study Group Report: Gravel Edition* (Washington, DC: Filiquarian Publishing, 2006), 9, 52, 55, 71, 72-76. Commonly known as the 'Iraq Study Group,' this report recommended a mix of an external approach to leverage regional powers like Syria and Iran (to responsibly encourage disaffected groups to reconcile), and an internal approach to make security force assistance the primary mission of American forces until withdrawal. Significantly, the report did not allow for additional troops since it saw their presence as the "direct cause for violence in Iraq."

[248] Frederick W. Kagan, *Choosing Victory: A Plan for Success in Iraq* (Washington, DC: American Enterprise Institute, 2006), 1.

[249] Ricks, *The Gamble*, 95-97. Keane's unofficial relationship with Petraeus and Odierno was unknown to Kagan at the time. Fortuitously, Odierno was already departing to take command of Multi-National Corps—Iraq, and Petraeus would soon follow to take command of the higher echelon, Multi-National Force—Iraq.

[250] Kagan, 1. After vetting the concepts and operational feasibility of the plan with then-Colonel H.R. McMaster and some of his veterans of the Tal Afar campaign, it was refined by a council of colonels in the Pentagon. AEI presented the concept to several congressional representatives, then President Bush reviewed the resulting proposal, enacting the strategy in January 2007.

[251] Ricks, *The Gamble*, Appendix B, Appendix C. *The Gamble* illustrates this contrast between the two approaches: Appendix B contains the brief Odierno received upon arrival in December 2006, and Appendix C contains Odierno's inbrief to Petraeus, dated 8 February 2007. When considered sequentially along with AEI's original concept in *Choosing Victory*, the transformation of the approach in Iraq takes shape.

> scale and outside of a few isolated examples; no one really had a good solution or way ahead. I thought the contribution that MNC-I made was instrumental. Even with [Petraeus]'s new guidance, I don't think we would have been successful if we would not have had [Odierno]'s operational concept.[252]

Similarly, Petraeus worked to ensure there was a sound linkage between the operational approach and the strategic end state from his command at MNF-I. He was able to place OIF in a larger regional context, to not only disrupt the transnational accelerants of instability, but to also fundamentally link Iraq back to its Arab neighbors. This is in stark contrast to the previous approach, which treated the campaign in isolation.[253] Concurrently, the tactical acumen of coalition and Iraqi Security Forces (ISF) commanders continued their steady adaptation. Intuition gained through multiple experiences in Iraq, unifying guidance, and updated doctrine all contributed to the increased capability to employ nuanced, coherent local measures for security and governance.[254]

However, it would be incorrect to solely attribute success in OIF to the actions of the security force itself. American forces and their ISF counterparts did not just ply the approach of *The Surge* against a complex background of varied conflict and confusing social structures; they were one and the same. Owing to the complex nature of hybrid warfare, all actors are interconnected through feedback and dynamic responses. As such, the population played at least as large a role in pulling Iraqi society back from the precipice of collapse. Two themes illustrate this best: the exhaustion of communal conflict and the reconciliation of extremist support bases.

By the time the additional resources and a unifying vision for *The Surge* kicked in, it was clear that the Shi'a had prevailed in the communal conflict in Baghdad, effectively leaving the Sunnis to question their role in the new Iraq.[255] From this position of disadvantage, Baghdad's Sunnis relied increasingly on AQI or other *takfiri* elements for security.[256] Almost concurrently, Sunnis in Al Anbar province to the west actively rejected AQI's attempts to consolidate power and over-extend their influence into the population's daily lives.[257] In what would come to be colloquially known as *The Awakening*,

---

[252] BH030, Interview. By virtue of his position on the MNF-I staff at the time, this respondent on the panel had direct knowledge of this planning effort. For clarity, the author substituted appropriate surnames for the callsigns and nicknames in the respondent's original quote.

[253] Ibid. This respondent had direct knowledge of Petraeus' efforts, owing to his experience in the MNF-I Initiatives Group.

[254] BA070, Battery Commander, Interview by Richard Johnson and Thomas Walton, Fort Leavenworth, KS, 24 February 2011; BA010, Interview. Several measures influenced this, primarily the organizational increase in tactical commanders' experience, but also the advent of an in-country repository for counterinsurgency adaptation and the application of refined doctrine. The Taji COIN Center provided a unique means of harmonizing operations, since all incoming units studied the commanders' intents from multiple levels of the counterinsurgency effort. One commander said that since he understood these intents, he could adapt methods to a changing environment in order to obtain that desired end state within his area. Doctrine encapsulated in Field Manual 3-24, *Counterinsurgency* was perhaps the largest institutional effect, since it provided a common concept and lexicon for all deploying forces and augmentees. However, this was more evolution than a revolution, as many practitioners in Iraq held the view that this doctrine simply distilled practices and concepts that were already widely in use when it was published in 2006.

[255] BH020, Interview.

[256] Kilcullen, *The Accidental Guerrilla*, 126-127.

[257] Sean MacFarland and Neil Smith, "Anbar Awakens: The Tipping Point," *Military Review* (March-April 2008): 42; BH040, Afghanistan Veterans Panel, Interview by Richard Johnson, Aaron Kaufman, Nathan Springer, and Thomas Walton, Washington, DC, 24 March 2011; Malkasian, "Counterinsurgency in Iraq:

then-Colonel Sean MacFarland and his Iraqi counterparts visualized operations that isolated insurgents to deny them sanctuary by: building the ISF through reconciled fighters, clearing and building combined combat outposts among the population, and engaging local leaders to determine which ones had the most local respect.[258] This successful integration of tribal forces into a security framework in Ramadi proved that Iraqis could remain armed to target the coalition's rivals and not descend into chaos.[259] An officer noted that it was like a wave of Sunni moderation emanating from Al Anbar, one which local commanders could exploit in Baghdad and the belts.[260]

Taken as a whole, the system engendered by *The Surge* begins to look like a list of ingredients: Petraeus and MNF-I's ability to unify effort in strategic context, Odierno and MNC-I's operational approach and focus on a spatially decisive action, the promulgation of refined security and development tactics, reconciliation techniques from *The Awakening* and operations in Ramadi, shape-clear-hold-build techniques from operations in Tal Afar, and finally the combat power to achieve it all.

Analysis

The operational approach in Iraq evolved with successive attempts to properly frame the complex environment, and eventually disrupted the hybrid threat's logic and form of violence. To bring in the familiar metaphor form our previous Vietnam case study, early attempts to address violence targeted the cape, not the toreador. Only through the purposeful application of improved intuition did the coalition learn to leverage the interconnected nature of conflict in Iraq, as a bull might become aware of the entire arena. Coalition forces benefitted from a maturing view of Iraqi conflict, a change in the internal logic for action in Baghdad and the belts, and the propensity within the system itself.

Initially, these efforts borrowed much from high value assets targeting by Special Operations Forces (SOF) which was crudely mimicked by conventional forces.[261] Some American units began to detain all military aged males in anti-coalition pockets because of a lack of actionable intelligence instead of killing or capturing specific leaders and facilitators.[262] Over time, these efforts began to focus more on the indirect

May 2003–January 2010," 303; McWilliams, 91. AQI viewed Ramadi as the future capital of its caliphate in Iraq and enjoyed relative freedom of movement in the area, making it almost exclusively denied terrain in the eyes of coalition forces. However, AQI had already worn out its welcome by late 2005, attempting to take over the lucrative smuggling routes to the west. One of the first groups (the Albu Issa tribe) to actively oppose them took its cue from these earlier efforts against AQI in Al Qaim (by the Abu Mahal tribe).

[258] MacFarland and Smith, 43; William Doyle, *A Soldier's Dream: Captain Travis Patrinquin and the Awakening of Iraq* (New York: NAL Caliber, 2011), 200-206. One factor that enabled this was the leeway given to an Army unit serving under a Marine headquarters, corroborated in interview with Interview BA010 (the respondent had direct knowledge of the planning and conduct of these operations in Ramadi).

[259] Panel discussion during U.S. Army Command and General Staff College Art of War Scholars Seminar, Iraq Session, 3 February 2011, Fort Leavenworth, KS.

[260] BC030, Battalion Commander; Interview by Benjamin Boardman and Richard Johnson, Fort Bragg, NC, 1 March 2011. The respondent operated in the Baghdad belts during this "wave of moderation" emanating from the west.

[261] Malkasian, "Counterinsurgency in Iraq: May 2003–January 2010," 290.

[262] Ricks, *Fiasco*, 224, 261, 280. These early efforts lacked focus; at one point in 2003 multiple intelligence analysts inside Abu Ghraib estimated that between 85% to 90% of all detainees sent there were of no intelligence

aspects of security rather than raids to kill or capture the few individuals actively fighting in the conflict. Additionally, commanders began to understand Iraq more in terms of Kilcullen's Venn diagram of interconnected hybrid warfare rather than discrete mission sets in which they prosecuted security actions in a closed system. As one squadron commander reflected on the approach in Tal Afar, "[w]e tried to switch the argument from Sunni versus Shi'a, which was what the terrorists were trying to make the argument, to Iraqi versus *takfirin*."[263] As with operations in Ramadi, reconciliation caused extremist groups to fundamentally alter their concepts of support, recruitment, logistics, and freedom of maneuver.[264]

The change in American forces' underlying approach in Baghdad and the belts further disrupted the hybrid threat's logic of violence. *The Surge* focused combat power to secure the population, which was not a key ingredient in past operations to deliberately clear or isolate areas. It is interesting to note that the *Jaysh al Mehdi* (JAM) did not adopt the same mix of regular and irregular forces seen in the attempts to clear Fallujah or Basra, or the early attempt to isolate Tal Afar. One possible explanation lies in the fact that the Shi'a initially viewed JAM as the only viable defenders of the population.[265] In combining American, ISF, and local security efforts, the population now had a sustainable alternative for security. Additionally, neighborhoods in the Baghdad area became increasingly homogenous as the communal violence peaked, owing to mass emigrations on both sides. When combined with American efforts to compartmentalize the city with physical barriers and checkpoints, the threat had to reconsider their ability to conduct attacks on anything but the security apparatus.[266]

Ironically, the propensity of the system itself may have provided the largest opportunity for disrupting the hybrid threat's logic of violence when one views events in Iraq through a wider aperture. AQI's drive to facilitate a sectarian conflict created a new dynamic within the system that coalition forces could exploit, but only briefly. Within an environment redefined with the additional aspect of communal violence, which was mostly absent prior to the 2006 bombing of the Golden Mosque in Samarra, the Coalition had a brief opportunity in the crisis to emplace population security, stabilize the environment, and come out in a position of advantage. Significantly, the shape-clear-hold-build framework signaled a resolve which made rivals reconsider their notion of exhausting the tactical force, just as *The Surge* made them question their ability to exhaust domestic America.

Over time, coalition forces learned to arrange tactical actions within the context that gave rise to the hybrid threat. Early operational art in Iraq was colored by the tenets of effects-based operations (EBO) and net-centric warfare (NCW), and in some ways the two theories were used as an insufficient substitute to arrange tactical actions instead

value. Units such as the 82d Airborne Division adapted and began to discriminate by screening, detaining over 3,800 Iraqis between August 2003 and March 2004 but only sending 700 to Abu Ghraib.

[263] Packer, "The Lesson of Tal Afar."

[264] Ricks, *The Gamble*, 210; BA010, Interview. *The Gamble* illustrates this point in the story of an AQI commander in Salah-ad'-Din province, whose captured diary from 2007 indicated that reconciliation reduced his strength from 600 fighters to only 20.

[265] BH030, Interview.

[266] Panel discussion during U.S. Army Command and General Staff College Art of War Scholars Seminar, Iraq Session, 3 February 2011, Fort Leavenworth, KS.

of a means to foster holistic views of complex systems. EBO constitutes an approach to targeting critical vulnerabilities in an adversary's system with lethal and nonlethal means in an attempt to achieve decisive effects through the defeat of presumably second-order capabilities. However, EBO was beset by the perception that it frames the environment from a detached perspective and overlays prescriptive categorization on the environment to assess action.[267] Similarly, NCW theory contended that networked information sharing leads to improved situational awareness, leading to collaboration and an improved ability to attack an adversary's network. Theoretically, NCW is an effective approach to a similarly networked enemy that is vulnerable to nodal disruptions, but this is based on a cybernetic nodal network instead of a biological network, one which may be more appropriate for complex social environments such as hybrid warfare in Iraq.[268] Both theories assume that an enemy is "mappable," a relatively inert system which neither anticipates nor preempts action.[269] Kagan asserts that while the military failed in pursuing transformation through EBO and NCW theories, at least the attempt to treat systems holistically indicates an advancing appreciation for complex warfare.[270]

Additionally, early efforts in Iraq lacked an adequate understanding of the environment. Initially, commanders did not understand the scope of action required in this form of warfare: "[y]our responsibilities are everything. And there was this false expectation that it would just fix itself."[271] Because of the aforementioned focus on security operations relying heavily on advantages in lethal firepower and force protection, American troops interacted with the populace from a defensive posture which effectively drove a psychological wedge between the people and their protectors.[272]

By distributing tactical operations and deploying combined forces among the populace, American forces gained the requisite context to align tactical actions in the same frame of reference which gave rise to the hybrid threat. The effect of combined American, ISF,

[267] James N. Mattis, "USJFCOM Commander's Guidance for Effects-Based Operations," *Parameters* 38, no. 3 (Autumn 2008): 18. EBO was effectively abandoned in 2008, with General Mattis' guidance for future dispensation of the model: "I am convinced that the various interpretations of EBO have caused confusion throughout the joint force and among our multinational partners that we must correct. It is my view that EBO has been misapplied and overextended to the point that it actually hinders rather than helps joint operations."

[268] Bousquet, 233-234; Cordesman, 54. Significantly, NCW pre-supposed eventual advances and proliferation of military networking technology, much in the same manner that early strategic air power advocates pre-supposed dominant advances in aircraft. Cordesman's assessment of IDF information sharing equipment in 2006 illustrates that modern forces do not have this capability yet, concluding that "A 'Net' is not a half-assed IT Dinosaur or a Failure Prone Toy."

[269] Antulio J. Echevarria II, *Rapid Decisive Operations: An Assumptions-based Critique* (Carlisle Barracks, PA: Strategic Studies Institute, 2001), 7-8.

[270] Frederick W. Kagan, *Finding the Target: The Transformation of American Military Policy* (New York: Encounter Books, 2006), xv, 393-397; William J. Gregor, "Military Planning Systems and Stability Operations," *Prism* 1, no. 3 (June 2010). Gregor's analysis is an even account regarding the role of organizational culture and competing agendas as the American military struggled to adapt planning systems (to include EBO and NCW) in an era of persistent hybrid and irregular warfare among the populace.

[271] AA510, Former DivArty Commander, Interview by Travis Moliere and Jesse Stewart, Fort Leavenworth, KS, 4 November 2010.

[272] Ricks, *Fiasco*, 221. Ricks illustrates this with a 2004 quote by then-Major General Peter Chiarelli, who at the time commanded the 1st Cavalry Division.

and local security allowed commanders to address the drivers of instability and conflict within the same context as their rivals, within their "way of war:"

> Indigenous forces have a lot of latitude that we don't have, they were not inhibited by ROE the way we were. It's rough justice…it's the messy and dark side of working with indigenous guys. You have to understand it and be willing to accept that. If you can live with that, and I can, then you're fine. If you're trying to change their culture and their way of war to be our way of war, then you'll be there a hell of a long time.[273]

In aligning areas of responsibility and spheres of influence with both ISF and local dynamics, American units could simultaneously address the immediate security issue and the underlying shortcoming with civil capacity.[274] Actions began to focus with a shared understanding between American forces and the local communities, enabling an eventual stimulation of local economies and a return to normalcy.[275] This focus on local solutions was a relative strength of coalition operations in OIF, as uniform country-wide solutions were widely avoided after the maligned De-Ba'athification effort in 2003.[276] In this, the utility of addressing rivals in a common environmental frame and developing tailored solutions becomes clear. As one officer described his unit's approach in Tal Afar:

> You can come in, cordon off a city, and level it, à la Falluja. Or you can come in, get to know the city, the culture, establish relationships with the people, and then you can go in and eliminate individuals instead of whole city blocks.[277]

Conclusion

Kilcullen's introduction to Iraq in *The Accidental Guerilla* aptly summarizes the complexity of developing an operational approach to hybrid warfare:

> If we were to draw historical analogies, we might say that operations in Iraq are like trying to defeat the Viet Cong (insurgency), while simultaneously rebuilding Germany (nation-building following war and dictatorship), keeping peace in the Balkans (communal and sectarian conflict), and defeating the IRA (domestic

[273] BA010, Interview.

[274] Panel discussion during U.S. Army Command and General Staff College Art of War Scholars Seminar, Iraq Session, 3 February 2011, Fort Leavenworth, KS.

[275] AA810, Battalion Commander, Interview by Ken Gleiman, Matt Marbella, Brian McCarthy, and Travis Molliere, Washington, DC, 13 September 2010; BH030, Interview. The latter, a Battalion Commander during this time in OIF added: "I could almost care less on who is JAM in my sector. You need to focus on the people who influence, use that information to inform the PRT [the Provincial Reconstruction Team]. What the bad guys were doing was almost irrelevant at that point."

[276] BF020, Interview; Gordon and Trainor, 564, 586-590. This *Cobra II* contains the ORHA briefing slides and the actual CPA order. Against the counsel of many Iraqis (to include secular Shi'a interim Prime Minister Iyad Allawi), the CPA declared that all Ba'ath Party members would be banned from holding senior in the army and government. This effectively dissolved most security forces, though a review of officer records indicated that only 8,000 of the 140,000 officers were committed Ba'athists. Collapsing the army also resulted in a mass of up to 400,000 military-aged males. Since Hussein's regime virtually required Ba'ath Party membership for any middle and upper class government job, there was an overwhelming dearth of civil service professionals. This directly contributed to the environment absent of effective local security in 2003, resulting in near-lawlessness that the American military simply could not address itself.

[277] Packer, "The Lesson of Tal Afar."

> terrorism). These all have to be done at the same time, in the same place, and changes in one part of the problem significantly affect others.[278]

Army units prevailed in much of these aspects through steady adaptation, resolve, and exploiting operational opportunities as part of an eventually unified coalition effort. In the context of this chapter's metaphor, coalition forces were able to disrupt the inherent logic in a school of piranhas, such that some of the piranhas turned on each other. This was a mix of both purposeful action and the inherent propensity within the social construct of Iraq. Although this operational approach resulted in end state conditions that achieved sufficient termination criteria, there will always be a degree of dissonance with the original concept of victory in Iraq as idealized in 2003. American forces undoubtedly left Iraq in a position of relative advantage and significant strategic gains in 2011, but the cost and efficacy of that advantage will surely be debated in the years to come.

As this monograph concludes, we must therefore analyze the utility of current doctrine to determine if it imparts sufficient flexibility to defeat hybrid threats and achieve that position of relative advantage. Specifically, what is an effective archetype for an operational approach in hybrid warfare, and does the *Unified Land Operations* model provide a sufficient lexicon and ideals to articulate such a construct? Because as costly and as strenuous as OIF was for the Army, the next hybrid threat could incorporate a similarly reflective effort to build its own effectiveness. As the Winograd Commission's final report succinctly captured this, "[w]hen speaking on learning, one should take into account enemies, too, are learning their lessons."[279]

6. Synthesis: Operational Approaches to Hybrid Warfare

> It is so damn complex. If you ever think you have the solution to this, you're wrong, and you're dangerous. You have to keep listening and thinking and being critical and self-critical.
>
> – Colonel H.R. McMaster, 2006

> Don't ever forget what you're built to do. We are built to solve military problems with violence.
>
> – Former Brigade Commander in OIF

This monograph began with an assertion that we gain a better context to develop operational approaches to hybrid threats by analyzing the U.S. Army's historical experience with hybrid warfare. Since the next adversary may guide its tactical efforts more coherently than the school of piranhas in Iraq, we therefore conclude with a review of the broad imperatives in hybrid warfare, an operational approach archetype, and a consequent evaluation of Unified Land Operations' ability to provide sufficient structure to these themes. The scope of this short study tempers any formal conclusion, since much more analysis is required to build confidence in the model described thus far. Hybrid warfare in Vietnam illustrates a deficiency in the three imperatives for operational approaches, while the Army's experience in OIF illustrates the adaptation to proficiency in all three imperatives. The resulting synthesis must avoid the temptation to highlight

[278] Kilcullen, 152.

[279] "Winograd Commission Final Report." *Council on Foreign Affairs*, accessed at: www.cfr.org/israel/winograd-commission-final-report/p15385 on 30 August 2011.

the contrasts between the two approaches, and cite only the principles in OIF as prescriptive keys to success in hybrid warfare. Using these imperatives to form the epitome of an operational approach reveals another inherent tension; one between the cognitive domain of understanding complex adaptive systems in hybrid warfare, and the physical domain of tactical efforts that leverage power relationships and violent action. The epigraphs above are perhaps the best illustration of this, from two commanders in OIF who were able to resolve this inherent tension in operational art.[280]

Three Imperatives for Operational Art in Hybrid Warfare

These explanatory fundamentals are not unique to hybrid warfare; they apply to all forms of warfare. However, the unique aspects of hybrid warfare merely illuminate three specific qualities in operational approaches, the broad methods that provide a basis to pursue strategic aims through the arrangement of tactical actions in time, space, and purpose. Operational approaches to hybrid warfare must cognitively disrupt the hybrid threat's logic in the forms of warfare it employs, arrange actions within the same context that gave rise to the hybrid threat, and avoid uniform or prescriptive means across time and space.[281]

The first of these imperatives could be considered the first among equals, since it generates and describes the need to *act* within the system of hybrid warfare. A well-grounded operational approach must cognitively disrupt the hybrid threat's logic in the forms of warfare it employs, rather than focusing on physical methods to counter the hybrid threat's means and capabilities. Operational art must produce articulated tactical actions and a unifying logic. Those actions must achieve this disruptive effect, creating an opportunity for further action. Effectively, this provides for the continuation of operations rather than a culmination. In Vietnam, MACV was unable to break the logic of *dau tranh*, which only became untenable to the Communist forces after their own operational over-reach in the Tet Offensive. In OIF, commanders leveraged their intuition of the environment to disrupt the rivals' logic for violence, creating opportunities via the ISF and local security forces.

Second, the approach must fuse tactical success to an overall strategic aim within the same context which gave rise to the hybrid threat. Fusion refers to the act of arranging tactical actions, and implies a conduit of success towards the strategic aim. But this transformative effort to address 'the gap' between the observed system and the desired system cannot take place in a frame which is artificially separate from the observed environment.[282] The American Army's approaches in Vietnam provide several cautionary lessons in this regard. Primarily, the military plans were self-referential, without sufficient regard for the social and political context of the war. The hybrid threat of Communist forces fundamentally viewed the war as a movement in social progress,

[280] This section's epigraphs are drawn from: Packer, "The Lesson of Tal Afar;" BA040, Brigade Commander, Interview by Aaron Kaufman and Dustin Mitchell, 23 February, 2011, Fort Leavenworth, KS.

[281] The requirement to arrange tactical actions in pursuit of a strategic aim is not listed as a distinct imperative to avoid redundancy, because by definition the operational approach is the broad, episodic employment of operational art in a specific context.

[282] Author's discussion with Israeli Diplomat, 7 March 2012, Jerusalem, Israel; Author's discussion with Retired IDF General Officer and Land Warfare Analyst, 8 March 2012, Latrun, Israel. The IDF's failure to consider the social and historical aspects which enabled Hezbollah's evolution is but one example of this.

not military confrontation; MACV lacked an appreciation for this rival narrative. In OIF, a growing appreciation for the environmental context of conflict enabled commanders to address the underlying accelerants of instability. The 2007 surge in troop strength was significant and enabled this effort, but it would not have been sufficient without an adaptive approach.

Lastly, an operational approach to hybrid warfare must avoid prescriptive or uniform measures across time and space. This is another acknowledgement that the environmental context in hybrid warfare is one of the chief characteristics of a relationally complex system. Since operational art must result in clear and concise guidance to arrange tactical actions, the operational approach cannot simply give commanders an appreciation for the complexity of the problem while dogmatically refusing to bound it. All guidance or unified effort will entail some degree of linearization or compartmentalization in order to clarify the environment, even through a simple narrative or order to subordinate echelons. This may be an immutable fact because sufficient clarity is required when aligning finite resources or combat power towards a specific purpose.[283] In Vietnam, MACV's pursuit of the *crossover point* provides an illustration of this. Within the effort to describe one unifying theme, the headquarters' intense focus on metrics such as the body count effectively precluded or stifled initiatives which were better adapted to local environments. OIF provides a positive example, as local solutions and distributed command models became the dominant model for both lethal and nonlethal efforts. These efforts were still harmonized by a common commander's guidance and doctrinal evolution, yet tactical commanders were able to develop internal measures of success.

An Archetype for Operational Approaches to Hybrid Warfare

The three preceding imperatives explain characteristics of an operational approach to hybrid warfare, but not a holistic approach. The question remains, how can an effective commander and his planning effort use these aspects to arrange tactical actions in hybrid warfare? The operational approach should be uniquely adapted to address 'the gap' that emerges in a comparison of the observed state and the desired end state. This monograph pre-supposes a hybrid threat in a spectrum of adversaries rather than as a categorical menu option, but this type of threat is specific enough to allow a focus on common aspects. Therefore, the question is not "what is the best operational approach to a hybrid threat?"; it should be, "given the characteristics of hybrid warfare, what does an effective operational approach to a hybrid threat 'look' like?"

From the imperative to cognitively disrupt the hybrid threat's logic in the forms of warfare it employs, there is a need to gain and maintain the initiative through continuous operations on a pathway to termination criteria. The requirement to utilize operational art within the same context which gave rise to the hybrid threat necessitates a focus on the overall environment, not simply an enemy. This also requires a commander and

[283] Peter M. Senge, *The Fifth Discipline: The Art and Practice of the Learning Organization* (New York: Doubleday, 2006), 72-73. Conversely, the employment of sound operational art should not impart additional complexity to the environment. Fighting complexity with complexity is actually the antithesis of holistic systems thinking, since it is more effective to understand the underlying dynamic interrelationships and address it with a simple solution. As such, the linearity of a solution is not a similarly ill-suited characteristic when compared to a solution's uniformity and prescriptiveness in hybrid warfare.

planner to see their force as an interconnected part of the overall environment, not as a detached spectator. Likewise, the imperative to avoid uniform or prescriptive solutions requires the approach to address the environment holistically, yet with appreciation to local variances.

These imperatives engender an archetype, not a stereotype. In this archetype, the combined action of shock and dislocation is the means to gain and maintain the initiative. Additionally, the operational approach must take special care to avoid a myopic view of the termination criteria and end state conditions for conflict.

Shock and Dislocation[284]

Operational shock reflects the notion that while it is impractical to destroy a hybrid threat's combat power in its entirety through attrition, a force can attack the coherent unity of the hybrid threat *as a system*.[285] If maneuver is conceived in purely linear terms, then spatial relationships become the dominant concern and a force may focus on issues like the amount of territory controlled, or the percentage of the population secured. However, if maneuver is conceived in the terms of Clausewitzian friction, nonlinear phenomena, and a holistic view of the environment, then an entire array of a rival's vulnerabilities avail themselves to attack.[286] In an ecology of logic, form, and function, striking the logic inherent in a hybrid threat's system is a realistic goal, whereas striking the entirety of a hybrid threat's already fragmented form is not. This partially illustrates the requirement for a harmonized effort in hybrid warfare, one that disrupts or defeats the interconnections in a rival's system rather than sequential search-and-destroy operations.[287] In other words, the very hybridity of this type of adversary introduces internal tensions in their mode of operation, and these tensions are an opportunity for action.[288] A hybrid threat's logic is an abstract cognitive quality, but it can be struck through both cognitive and physical means.[289] For example, coalition forces in OIF shocked the metaphoric school of piranhas by developing local security forces. This not only enabled

[284] Headquarters, Department of the Army, *Field Manual 100-5: Operations* (Washington, DC: Department of the Army, 1982), page 2-2. This discussion of shock and dislocation is not a unique concept, rather an amalgam of existing theory. For example, the 1982 version of AirLand Battle doctrine provides a similar exhortation: . "…we must make decisions and act more quickly than the enemy to disorganize his forces and to keep him off balance."

[285] Naveh, *In Pursuit of Military Excellence*, 16-17; Paul J. Blakesley, *Operational Shock and Complexity Theory* (master's thesis, School of Advanced Military Studies, 2005), 68-69. This assertion must be considered with the additional insight that the actor, the force attempting to strike a hybrid threat to induce operational shock, is also profoundly interconnected in the same system of warfare.

[286] Ofra Gracier, *Between the Feasible and the Fantastic: Orde Wingate's Long-Range Penetration—A Spatial View of the Operational Manoeuvre* (doctoral dissertation, Tel Aviv University, 2008), 48-49.

[287] Naveh, "The Cult of the Offensive Preemption," 182. Israeli maneuver theorist Shimon Naveh develops this concept of an operational strike further, describing three chief components: "*fragmentation*—aimed at preventing the horizontal synergy among the components of the rival system from materializing; *simultaneous action* by the elements of the friendly system along the entire physical and cognitive depth of its rival's layout in an attempt to disrupt the hierarchical interaction among its various elements; and *momentum*, predicated on the initiation of a successive chain of tactical actions, guided by a single aim and operating within the decision-action loop of the rival system."

[288] Author's discussion with Israeli Military Analyst, 8 March 2012, Tel Aviv, Israel.

[289] Blakesley,18-19, 73. A combat operation which induces operational shock not only changes the physical vestiges of the environment from the enemy's point of view, it also fundamentally changes the nature of the problem the enemy commander or command structure faces. This indelibly pushes the enemy's system towards a chaotic state, which in more colloquial terms may represent 'dissolution' or 'collapse.'

lethal direct attacks on the rivals' combat power, resources, and networks, it also fundamentally changed the nature of the problem they faced. This also demonstrates how operational shock creates opportunities in the redefined environment, as one brigade commander reflected that these operations supported his overall theme of exploiting success to keep the initiative.[290] However, if the objective of operational shock is to neutralize the enemy's will to continue the conflict in pursuit of an aim, shock is not sufficient alone since the hybrid threat is less likely to serve extrinsic state-defined goals. As such, there must be a complementary effort to render the rival's current form of warfare irrelevant, a mechanism to defeat it.

One way to pursue a relative defeat of the enemy's remainder is through dislocation, "the art of rendering the enemy's strength irrelevant."[291] In other words, a force cannot defeat all of a hybrid threat's military, political, and social strength but it can change the environment so that the enemy's remaining strength is of negligible value to him.[292] Hart, Boyd, and Osinga develop the assertion that dislocation springs from the enemy's fundamental sense of surprise as a result of purposeful action.[293] In this lies the bridge between shock and dislocation, as their efforts should exhibit a reflexive quality: shock creates this sense of surprise, and dislocation presents itself in an opportunity.[294] Furthermore, when dislocation seems sudden, it results in a sense of being "trapped."[295] To continue the OIF example, the shock of a redefined environment dislocated the existing elements of combat power as rivals understood them, rendering their remaining power mostly irrelevant and trapped in an area which could be marginalized.[296] Conversely, it is doubtful that Hezbollah felt psychologically trapped in southern Lebanon in 2006, or if Communist forces ever felt trapped in SVN.[297]

---

[290] BA010, Interview; Author's discussion with Israeli Military Analyst, 9 March 2012, Tel Aviv, Israel. In the Israeli experience, Hezbollah reorganized very clearly once the IDF could maintain contact with their forces on the ground, availing additional opportunities for action.

[291] Leonhard, 66.

[292] Headquarters, Department of the Army, *Field Manual 3-0: Operations* (*Incl. Change 1)* (Washington, DC: Department of the Army, 2011), page 7–7. This discussion casts dislocation with respect to functional relationships, a departure from the traditional military view of dislocation with respect to spatial relationships: "Dislocate means to employ forces to obtain significant positional advantage, rendering the enemy's dispositions less valuable, perhaps even irrelevant. It aims to make the enemy expose forces by reacting to the dislocating action. Dislocation requires enemy commanders to make a choice: accept neutralization of part of their force or risk its destruction while repositioning."

[293] B.H. Liddell Hart, *Strategy* (London: Faber and Faber, 1967), 323–325; John Boyd, *Patterns of Conflict* (unpublished presentation), 98, 115; Osinga, 34–35.

[294] Author's discussion with Retired IDF General Officer and Member of the Winograd Commission, 8 March 2012, Tel Aviv, Israel. One example of this could arise in a sequel to the 2006 war; as Hezbollah transforms its military to a more hierarchical system in the wake of the conflict, approaches like High Value Target (HVT) methodology may be considerably more effective in disrupting their new logic after the initial operational shock of 2006. Although it is pure conjecture, this opportunity may have emerged had the 2006 war lasted longer than 34 days.

[295] Hart, 327.

[296] Ricks, *The Gamble*, 210. The account of the AQI leader in Salah-ad'-Din cited in the previous chapter provides one example of this. Few, if any, unclassified sources describe or analyze a similar mindset among AQI leaders in Fallujah or Tal Afar (roughly 2004), much less JAM leaders in Sadr City (2007–2008) or Basra (2009). However, it is likely they felt a similar sense of being trapped. Although a hybrid threat's individual elements can always find at least one physical rat-line out of town, the utility of dislocation lies in this being trapped in a psychological sense, not a physical sense.

[297] Headquarters, Department of the Army, *Field Manual 3-0: Operations (Incl. Change 1)*, pages 7–6 to 7–8. In the course of this study, the other three U.S. Army doctrinal defeat mechanisms were analyzed for

Avoiding End State Myopia

Shock and dislocation describe the effect of concrete tactical actions, while an effort to avoid end state myopia reflects the abstract strategic context.[298] As this monograph highlights, the inherent tension between these two domains is one of the principle difficulties in applying operational art. However, commanders and planners must maintain a long view because operations and strategy exhibit a reflexive relationship.[299] Initial actions change the environment, so the pathway to conflict termination and the conception of the end state change as well.

If operational art provides for continuity instead of culmination, then a force must reconcile with the notion that it will not defeat a hybrid threat in one single maelstrom of genius and concerted violence. Hence, shock and dislocation apply in a complementary fashion. This also illustrates the utility in phasing operations, to extend operational reach over time toward several objectives and decisive points. One hedge against a myopic view of the end state is a continuous effort to analyze operational objectives, to determine if they constitute conflict termination or solely a decisive point which gains a marked advantage over the adversary. Hybrid warfare exhibits supradomain combinations of political and social aspects, operationalized in irregular warfare. Therefore, the operational approach must incorporate these decisive points along the metaphoric pathway towards conflict termination, with respect to the political and social grievances instead of focusing on a purely military-security end state and relying on the rest of the environment to self-correct. As one former officer who served in the Gulf War recalled, "everybody thought that the thing was over. I find that as one expression of this tendency to think that good operations fix the problem and that therefore there's no need to think beyond when the shooting stops."[300]

The Sufficiency of Operational Art in Unified Land Operations

As AirLand Battle doctrine had a specific threat and strategic context to address, Unified Land Operations characterizes the hybrid threat as the chief form of adversary the U.S. Army is most likely to face in the near-term. Significantly, it describes this threat in terms of synergy and protracted warfare.[301] Maneuver on land is not solely intended to

---

their utility in hybrid warfare. Destruction through a single decisive attack is highly unlikely to present itself in the course of hybrid warfare. The sequential application of destruction, attrition, is not a viable option to defeat the hybrid threat, as seen in the previous case studies. In any case, this defeat mechanism will prompt a cost-benefit analysis by the hybrid threat to continue conflict, which may be summarily resumed once combat power is regenerated. Isolation may be a useful local tactic, but is nearly impossible in both physical and cognitive terms in a war including irregular forces distributed among the populace. Consequently, disintegration is another ill-suited defeat mechanism owing to its reliance on prior destruction or isolation.

[298] The term "end state myopia" first appears as a metaphoric affliction of commanders in: Steven Rotkoff, "Introspection and Emotional Vulnerability as Leader Development and Team Building Tools," *Small Wars Journal*, www. smallwarsjournal.com/blog/journal/docs-temp/777-rotkoff.pdf (accessed 13 December 2011).

[299] Author's discussion with Israeli Strategist, 7 March 2012, Jerusalem, Israel. This imperative becomes increasingly important because American forces will almost always face questions of legitimacy from a rival organization during expeditionary operations, much like Israeli forces in 2006.

[300] BF010, Interview.

[301] Headquarters, Department of the Army, *Army Doctrinal Publication 3-0: Unified Land Operations*, 4.

occupy the adversary's territory.[302] To this end, doctrine must provide an orientation to the force, especially given the high conversion cost between primarily regular warfare and primarily irregular warfare. To achieve this, Unified Land Operations discusses warfare through the lens of initiative and a full spectrum of operations.

French Enlightenment and reductionist thought informed Jominian military theory, German Rationalism informed Clausewitzian military theory, and contemporary thought improves efforts in conceptual planning. In many ways, Unified Land Operations aligns itself with the emerging understanding of the world through nonlinear sciences, epistemological and ontological foundations.[303] In this, Unified Land Operations has great utility. The model of gaining and retaining the initiative through a spectrum of operations by the complementary means of CAM and WAS is one that commanders at all echelons can understand and leverage against complex systems in hybrid warfare. Significantly, the doctrine calls for articulated solutions to arrange tactical actions.[304] Tactical commanders require this clarity to give their actions purpose and ensure they understand their role within the higher commander's greater unifying logic to defeat a hybrid threat. Operational planners owe them a clear framework with at least this much.

Closing: Leveraging Legitimate Violence

Through a deeply critical process, the commander and his planners may come to a greater understanding of the unique ecology of the complex hybrid threat they face: its form, its function, and its logic for violence. Arranging a specific tactical action should affect one aspect of this ecological trinity, lest the operational approach become too complex. A complicated, yet manageable solution is preferable.[305] Therein lies the rub for operational planners, and a caution against purely cognitive or abstract solutions. There is a significant difference between useful tools for conceptual planning, and useful tools for coordinating and synchronizing complicated tactical actions.[306] In 2006, a general on Halutz's staff spoke of disrupting the logic of Hezbollah and creating a "spectacle of victory" in Bint J'beil, leaving many tactical commanders to wonder exactly what he meant.[307] The successful operational approach blends a holistic understanding of hybrid warfare with an appreciation for what the organization is structured to do, and its ability to adapt. It must be able to guide legitimate violence, or the threat

[302] Author's discussion with Retired IDF General Officer and Land Warfare Analyst, 8 March 2012, Latrun, Israel. Conversely, land maneuver should convince the adversary that its position is one of a relative disadvantage, given a continuous arrangement of the force's tactical victories.

[303] Dolman, 96-100; Bousquet, 189-191. This relationship between the three respective modes of thought and contemporaneous military theory was brought to the author's attention during a seminar discussion by Major James Davis, Australian Army.

[304] Headquarters, Department of the Army, *Army Doctrinal Publication 3-0: Unified Land Operations*, 10.

[305] Department of Defense Joint Staff, *Planner's Handbook for Operational Design* (Suffolk, VA: Joint Staff J-7, 2011), II-5, II-8—II-9. This reflects the difference between a system or solution which is interactively complex (what we see as truly complex or nonlinear) and one which is structurally complex (what we see as merely complicated or linear).

[306] Author's discussion with Israeli Military Analyst, 9 March 2012, Tel Aviv, Israel. Despite the IDF's perceived predilection for SOD, this analyst succinctly asserted that it is a conceptual planning tool and not a method for coordination and synchronization.

[307] Bar-Joseph, 154, 156-157; Sultan, 54, 56; Harel and Issacharof, 119-120, 126-128, 136-139; Matthews, *We Were Caught Unprepared*, 45.

of legitimate violence. This is supremely difficult, but then again "nobody pays to see a guy juggle one ball."[308]

This effort must pervade the operational approach to hybrid warfare, ensuring that it incorporates the three imperatives discussed above with a holistic understanding of the threat and environment. Hybrid threats will undoubtedly continue to seek the synergistic effect of regular and irregular qualities in order to protract the conflict. They will wage warfare in a resilient manner which is *built to last*. The U.S. Army can effectively counter this if its operational approaches to hybrid warfare utilize shock and dislocation along a pathway to conflict termination; it must address the gap between the current state and the desired end state in a manner which is *built to outlast*.

[308] Attributed to Colonel Patrick Roberson, who used this as an illustration of the inherent complexity in warfare during a discussion with the author.

DOCUMENT NO. 3

HYBRID WARFARE

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 10, 2010

The Honorable Loretta Sanchez
Chairwoman
The Honorable Jeff Miller
Ranking Member
Subcommittee on Terrorism, Unconventional Threats and Capabilities
Committee on Armed Services
House of Representatives

The Honorable Adam Smith
House of Representatives

Subject: *Hybrid Warfare*

Senior military officials recently testified[1] before Congress that current and future adversaries are likely to use "hybrid warfare" tactics, a blending of conventional and irregular approaches across the full spectrum of conflict. In addition, several academic and professional trade publications have commented that future conflict will likely be characterized by a fusion of different forms of warfare rather than a singular approach. The overarching implication of hybrid warfare is that U.S. forces must become more adaptable and flexible in order to defeat adversaries that employ an array of lethal technologies to protracted, population-centric conflicts such as those in Iraq and Afghanistan. Department of Defense (DOD) officials have discussed the need to

[1] *Hearing on U.S. Southern Command, Northern Command, Africa Command, and Joint Forces Command Before the House Armed Services Committee*, 111th Cong. (2009) (statement of General James N. Mattis, USMC Commander, United States Joint Forces Command); *Hearing on the Fiscal Year 2011 National Defense Authorization Budget Request for Department of Defense's Science and Technology Programs Before the Subcommittee on Terrorism, Unconventional Threats and Capabilities of the House Armed Services Committee*, 111th Cong. (2010) (statement of Rear Admiral Nevin P. Carr, Jr., United States Navy Chief of Naval Research); and *Hearing on U.S. Marine Corps Readiness Before the Subcommittee on Defense of the House Committee on Appropriations*, 110th Cong. 132-133 (2008) (testimony of Lieutenant General James F. Amos, Deputy Commandant of the Marine Corps for Combat Development and Integration).

counter the continuum of threats that U.S. forces could face from non-state- and state-sponsored adversaries, including computer network and satellite attacks; portable surface-to-air missiles; improvised explosive devices; information and media manipulation; and chemical, biological, radiological, nuclear, and high-yield explosive devices.

In light of references to "hybrid warfare" by senior military officials and possible implications it could have for DOD's strategic planning, you requested we examine: (1) whether DOD has defined hybrid warfare and how hybrid warfare differs from other types of warfare and (2) the extent to which DOD is considering the implications of hybrid warfare in its overarching strategic planning documents. On June 16, 2010, we met with your staff to discuss the preliminary results of our work. This report formally transmits our final response to your request.

Scope and Methodology

To determine how DOD defines hybrid warfare, how hybrid warfare differs from other types of warfare, and how DOD uses the concept in its strategic planning documents, we reviewed and analyzed DOD doctrine, guidance, policy, and strategic planning documents, and interviewed Office of the Secretary of Defense (OSD), Joint Staff, service headquarters, Defense Intelligence Agency, and combatant command officials. More specifically, our review and analysis included the most recent *National Defense Strategy*; the 2010 *Quadrennial Defense Review Report*; and the 2010 *Joint Operating Environment*.

We conducted this performance audit from January 2010 to September 2010 in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

Senior military officials in recent public testimony asserted the increased likelihood of U.S. forces encountering an adversary that uses hybrid warfare tactics, techniques, and procedures. However, DOD has not officially defined hybrid warfare at this time and has no plans to do so because DOD does not consider it a new form of warfare. Rather, officials from OSD, the Joint Staff, the four military services, and U.S. Joint Forces Command told us that their use of the term hybrid warfare describes the increasing complexity of future conflicts as well as the nature of the threat. Moreover, the DOD organizations we met with differed on their descriptions of hybrid warfare. For example, according to Air Force officials, hybrid warfare is a potent, complex variation of irregular warfare. U.S. Special Operations Command officials, though, do not use the term hybrid warfare, stating that current doctrine on traditional and irregular warfare is sufficient to describe the current and future operational environment.

Although hybrid warfare is not an official term, we found references to "hybrid" and hybrid-related concepts in some DOD strategic planning documents; however, "hybrid warfare" has not been incorporated into DOD doctrine. For example, according to OSD officials, hybrid was used in the 2010 *Quadrennial Defense Review Report* to draw attention to the increasing complexity of future conflicts and the need for adaptable, resilient

U.S. forces, and not to introduce a new form of warfare. The military services and U.S. Joint Forces Command also use the term "hybrid" in some of their strategic planning documents to articulate how each is addressing current and future threats, such as the cyber threat; however, the term full spectrum often is used in addition to or in lieu of hybrid.

Agency Comments

We provided a draft of this report to DOD. DOD reviewed the draft report and concurred with the information presented in the report. DOD's comments are reprinted in their entirety in enclosure II.

- - - - -

We are sending copies of this report to the appropriate congressional committees. We are also sending a copy to the Secretary of Defense. In addition, this report will be available at no charge on our Web site at http://www.gao.gov/. Should you or your staff have any questions concerning this report, please contact me at (202) 512-5431 or dagostinod@gao.gov or Marc Schwartz at (202) 512-8598 or schwartzm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report.

Key contributors to this report include Marc Schwartz, Assistant Director; Jennifer Andreone; Steve Boyles; Richard Powelson; Kimberly Seay; and Amie Steele.

[Signature]

Davi M. D'Agostino
Director
Defense Capabilities and Management

Enclosures

Hybrid Warfare

Briefing to the
Subcommittee on Terrorism, Unconventional Threats and Capabilities,
Committee on Armed Services, House of Representatives

September 10, 2010

GAO-10-1036R

Overview

- Introduction
- Key Questions
- Scope and Methodology
- Summary
- Background
- Observations
- Agency Comments
- Enclosure I: DOD Definitions of Warfare
- Enclosure II: Comments from the Department of Defense

Introduction

- Senior military officials used the term "hybrid warfare" during testimony before Congress between 2008–2010 to describe the methods used by U.S. adversaries in Iraq and Afghanistan, and what U.S. forces are likely to encounter in future conflicts.
- Moreover, many academic and professional trade publications have commented that future conflict will likely be characterized by a fusion of different forms of warfare rather than a singular approach.
- Hybrid warfare tactics consist of the blending of conventional, unconventional, and irregular approaches to warfare across the full spectrum of conflict.

Key Questions

In response to your request, our objectives in this review were to determine:

1. Whether DOD has defined hybrid warfare and how hybrid warfare differs from other types of warfare.

2. The extent to which DOD is considering the implications of hybrid warfare in its overarching strategic planning documents.

We conducted this review from January 2010 to September 2010 in accordance with generally accepted government auditing standards.

Scope and Methodology

- To determine whether DOD has defined or intends to define hybrid warfare and how hybrid warfare is different from other types of warfare, we examined DOD-approved definitions of warfare—such as irregular and unconventional warfare—and compared them with the concept of hybrid warfare. We also met with Office of the Secretary of Defense (OSD), Joint Staff, service headquarters, Defense Intelligence Agency, and combatant command officials to obtain their perspectives on the term and determine whether they have formally defined it (see pages 6–7).
- To determine the extent to which DOD is considering the implications of hybrid warfare in its overarching strategic planning documents, we reviewed and analyzed DOD strategies, doctrine, guidance, and policies, including the 2008 *National Defense Strategy*,[1] the 2010 *Quadrennial Defense Review Report*,[2] the 2010 *Joint Operating Environment*,[3] and the 2009 *Capstone Concept for Joint Operations*.[4] We also discussed this matter with DOD officials from the organizations listed on pages 6–7.

We met with officials from the following DOD organizations:

- The Joint Staff, Joint Force Development and Integration Division
- Office of the Assistant Secretary of Defense, Special Operations/Low Intensity Conflict & Interdependent Capabilities, Office of Special Operations & Combating Terrorism
- Office of the Under Secretary of Defense for Policy, Force Development
- Office of the Under Secretary of Defense, Comptroller
- Office of the Secretary of Defense, Cost Assessment and Program Evaluation
- Defense Intelligence Agency
- U.S. Joint Forces Command
  - o Joint Irregular Warfare Center
  - o Joint Futures Group
  - o Joint Center for Operational Analysis
  - o Joint Training and Joint Warfighting Center Directorate
  - o Joint Concept Development and Experimentation Directorate
- U.S. Special Operations Command
  - o Operational Plans and Joint Force Development Directorate
  - o Joint Capability Development Directorate

[1] United States Department of Defense, *National Defense Strategy* (Washington, D.C., June 2008).

[2] United States Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C., February 2010).

[3] United States Joint Forces Command, *The Joint Operating Environment* (Suffolk, Va., February 2010).

[4] United States Department of Defense, *Capstone Concept for Joint Operations, Version 3.0* (Washington, D.C., January 2009).

  - Joint Concept Development and Experimentation Directorate
  - Strategic Plans and Policy Directorate
- U.S. Army Headquarters
  - Office of the Deputy Chief of Staff for Operations and Plans
  - Office of the Deputy Chief of Staff for Intelligence
- U.S. Army Training and Doctrine Command
- U.S. Air Force Headquarters
  - Irregular Warfare Requirements Directorate
- U.S. Navy Headquarters
  - Navy Irregular Warfare Office
- U.S. Marine Corps Headquarters
  - Marine Corps Combat Development Command, Concepts and Plans

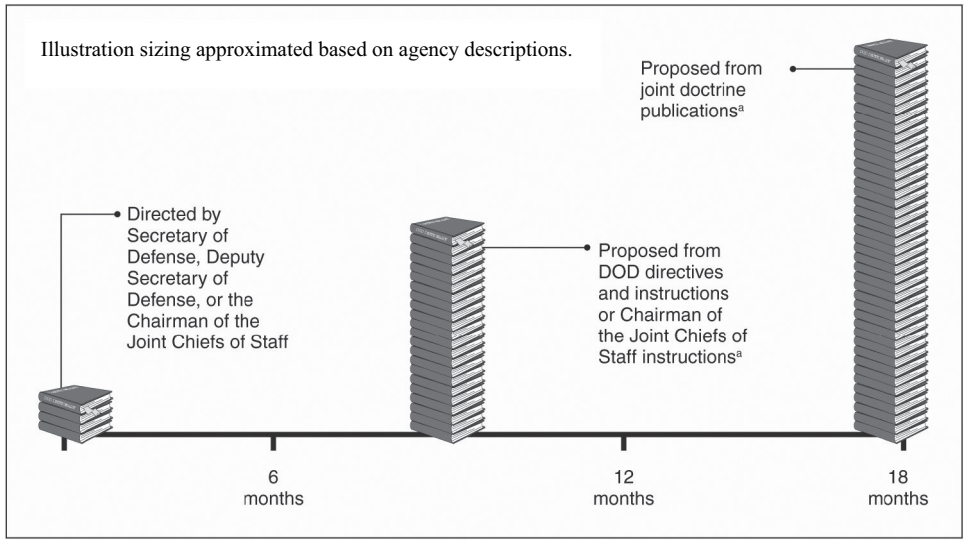
Summary

- DOD has not officially defined "hybrid warfare" at this time and has no plans to do so because DOD does not consider it a new form of warfare.
- DOD officials from the majority of organizations we visited agreed that "hybrid warfare" encompasses all elements of warfare across the spectrum. Therefore, to define hybrid warfare risks omitting key and unforeseen elements.
- DOD officials use the term "hybrid" to describe the increasing complexity of conflict that will require a highly adaptable and resilient response from U.S. forces, and not to articulate a new form of warfare.
- The term "hybrid" and hybrid-related concepts appear in DOD overarching strategic planning documents (e.g., 2010 *Quadrennial Defense Review Report*); however, "hybrid warfare" has not been incorporated into DOD doctrine.

Background

- *Department of Defense Dictionary of Military and Associated Terms* (Joint Publication 1-02), sets forth standard U.S. military and associated terminology that, together with their definitions, constitutes approved DOD terminology. There are approximately 6,000 terms in Joint Publication 1-02.
- Chairman of the Joint Chiefs of Staff Instruction 5705.01C, *Standardization of Military and Associated Terminology*, stipulates four methods to add, modify, or delete DOD terminology in Joint Publication 1-02.
- As shown in figure 1, according to Joint Staff officials, the approval process to incorporate a new term in Joint Publication 1-02 can take place immediately to approximately 18 months. The majority of approved terms are proposed due to their inclusion in existing joint doctrine publications.

Figure 1: Methods to Incorporate New DOD Terminology into Joint Publication 1-02



Source: GAO analysis of DOD's terminology approval process.

[a] The fourth method to incorporate a new term into Joint Publication 1-02 is through terminology proposed from the *NATO Glossary of Terms and Definitions (English and French),* which may be proposed for adoption and inclusion by the Department of Defense in the appropriate Joint Publication, Chairman of the Joint Chiefs of Staff Instruction, or DOD document.

Observations
Objective 1: Definition

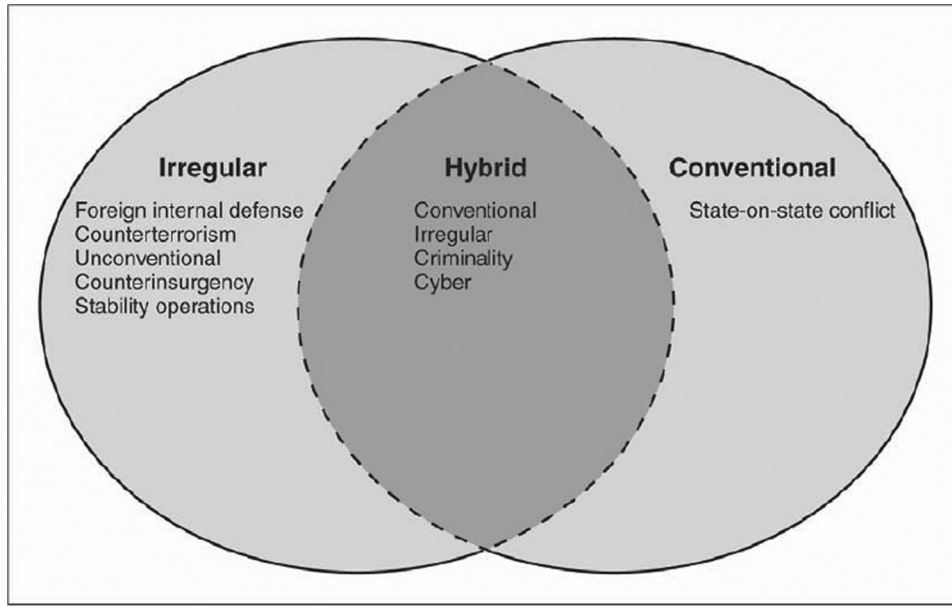
- DOD has not formally defined hybrid warfare at this time and does not plan to do so because DOD does not consider it a new form of warfare.
- DOD officials indicated that the term "hybrid" is more relevant to describe the increasing complexity of conflict that will require a highly adaptable and resilient response from U.S. forces rather than a new form of warfare.
- DOD officials have different characterizations of recent conflicts. For example:
  - o Air Force officials stated that the conflicts in Iraq and Afghanistan are irregular warfare and hybrid, while Army and Navy officials both considered Afghanistan irregular warfare and Iraq initially conventional warfare and then later, irregular warfare.
  - o U.S. Special Operations Command and Army officials characterized the Russia-Georgia conflict as conventional warfare, while Air Force officials considered it a hybrid conflict.
- Discussions about hybrid *threats*, as opposed to hybrid warfare, are ongoing within DOD; however, most of the DOD officials whom we spoke with stated that it was premature to incorporate hybrid threats into doctrine.

- The North Atlantic Treaty Organization (NATO) has defined hybrid threat as follows, and is developing doctrine on countering the hybrid threat.
  - o "A hybrid threat is one posed by any current or potential adversary, including state, non-state and terrorists, with the ability, whether demonstrated or likely, to simultaneously employ conventional and non conventional means adaptively, in pursuit of their objectives."[5]

Objective 1: The Hybrid Warfare Concept

According to our analysis of DOD and academic documents, hybrid warfare *blends* conventional[6] and irregular warfare[7] approaches across the full spectrum of conflict. Figure 2 displays a sample of approaches that could be included in hybrid warfare.

Figure 2: The Hybrid Warfare Concept



Source: GAO analysis of DOD military concept and briefing documents and academic writings.

[5] This definition was approved by the NATO Military Working Group (Strategic Planning & Concepts), February 2010.

[6] The *Irregular Warfare Joint Operating Concept*, v. 1.0, defines conventional warfare as a form of warfare between states that employs direct military confrontation to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory in order to force a change in an adversary's government or policies. Conventional warfare may also be called "traditional" warfare. Conventional warfare is not defined in Joint Publication 1-02.

[7] Joint Publication 1-02 defines irregular warfare as a violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will.

Objective 1: Definition Comparison

- DOD officials have differing views on whether or how hybrid warfare differs from other types of warfare.[8]
  - o According to Air Force officials, hybrid warfare is more potent and complex than irregular warfare due to increased tempo, complexity, diversity, and wider orchestration across national borders, which are all exacerbated by the ease with which adversaries can communicate, access international resources and funding, and acquire more lethal and sophisticated weaponry.
  - o Special Operations Command officials stated that hybrid warfare is no different from current doctrinal forms of warfare employed across the spectrum of conflict.
  - o Navy officials stated that hybrid is synonymous with full spectrum and encompasses both conventional warfare and unconventional warfare.
  - o Marine Corps officials use the term "hybrid" to describe the potential threat posed by both state and non-state actors and believe that hybrid warfare is not a new form of warfare; rather it is synonymous with full spectrum conflict and is already adequately covered in current doctrine.

Objective 1: Unofficial Definitions

The following are examples of unofficial definitions of hybrid warfare/threat that we found in military concept and briefing documents and in academic writings (emphases added):

> ***Hybrid Warfare***—Conflict executed by either state and/or non-state threats that employs **multiple modes of warfare** to include conventional capabilities, irregular tactics, and criminal disorder. (U.S. Joint Forces Command, Joint Center for Operational Analysis briefing on "Joint Adaptation to Hybrid War")
>
> ***Hybrid Threat***—An adversary that simultaneously and adaptively employs some **fused combination** of (1) political, military, economic, social and information means and (2) conventional, irregular, terrorism and disruptive/criminal conflict methods. It may include a combination of state and non-state actors. (Working definition derived by U.S. Joint Forces Command, Joint Irregular Warfare Center, 2008–2009)
>
> ***Hybrid Threat***—A threat that simultaneously employs regular and irregular forces, including terrorist and criminal elements to achieve their objectives using an **ever-changing variety of conventional and unconventional tactics** to create multiple dilemmas. (U.S. Army Training and Doctrine Command's Operational Environment, 2009–2025)
>
> ***Hybrid Threats***—Threats that incorporate **a full range of different modes of warfare** including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both states and a variety of non-state actors.[9]

[8] The Joint Publication 1-02 definitions of types of warfare are listed in enclosure I.

[9] Lt. Col. Frank G. Hoffman, U.S. Marine Corps Reserve (Ret.), *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, Va.: Potomac Institute for Policy Studies, 2007), p.8.

Objective 2: Strategic Planning

- DOD uses the term "hybrid" in select strategic planning documents to articulate how it is addressing current and future threats. For example:
  - The term "hybrid" is mentioned twice in the 2010 *Quadrennial Defense Review Report* to describe the approaches and capabilities that potential adversaries may use against U.S. forces and counteractions DOD can take.
  - The term "hybrid" is used in the 2010 *Joint Operating Environment* to describe the combination of lethal technology and the protracted, population-centric nature of contemporary and future conflicts.
  - The 2009 *Capstone Concept for Joint Operations* states that future conflicts will appear as hybrids comprising diverse, dynamic, and simultaneous combinations of organizations, technologies, and techniques that defy categorization.
  - The 2010 *Army Modernization Strategy*[10] states that the Army must continue to upgrade its capabilities to remain a dominant force and successful against hybrid threats, global terrorists, and followers of extremist ideologies.
- Some DOD organizations have adopted the term "full spectrum operations" in addition to or in lieu of the term "hybrid."
  - The 2010 *Army Posture Statement*[11] uses the term "full spectrum operations"[12] in addition to hybrid threats to describe current and future military operations.
  - According to Army officials, full spectrum operations underpin both conventional and irregular warfare.
  - The *Air Force Global Partnership Strategy*[13] states that as the United States fights insurgencies and terrorism, the U.S. Air Force must maintain its capacity to conduct full spectrum operations to defeat U.S. enemies in operations of traditional and irregular character.

Agency Comments

- We provided a draft of this report to DOD.
- DOD reviewed the draft report and concurred with the information presented in the report.
- DOD comments are reprinted in their entirety in enclosure II.

[10] United States Department of the Army, *Army Modernization Strategy* (April 2010).

[11] United States Department of the Army, *Army Posture Statement*, "America's Army: The Strength of the Nation" (February 2010).

[12] Army Field Manual No. 3-0, *Operations*, defines full spectrum operations as an operational concept in which Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results.

[13] United States Air Force, *Air Force Global Partnership Strategy: Building Partnerships for the 21st Century* (December 2008).

Enclosure I: DOD Definitions of Warfare

Department of Defense Dictionary of Military and Associated Terms (Joint Publication 1-02), includes the following definitions of warfare:[14]

Acoustic Warfare (DOD, NATO) Action involving the use of underwater acoustic energy to determine, exploit, reduce, or prevent hostile use of the underwater acoustic spectrum and actions which retain friendly use of the underwater acoustic spectrum.

Antisubmarine Warfare (DOD, NATO) Operations conducted with the intention of denying the enemy the effective use of submarines.

Atomic Warfare (DOD, NATO) See nuclear warfare.

Biological Warfare (DOD, NATO) Employment of biological agents to produce casualties in personnel or animals, or damage to plants or materiel; or defense against such employment.

Chemical Warfare (DOD) All aspects of military operations involving the employment of lethal and incapacitating munitions/agents and the warning and protective measures associated with such offensive operations. Since riot control agents and herbicides are not considered to be chemical warfare agents, those two items will be referred to separately or under the broader term "chemical," which will be used to include all types of chemical munitions/agents collectively.

Directed-Energy Warfare (DOD) Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum.

Electronic Warfare (DOD) Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support.

Guerrilla Warfare (DOD, NATO) Military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces.

Irregular Warfare (DOD) A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, in order to erode an adversary's power, influence, and will.

Land Mine Warfare (DOD, NATO) See mine warfare.

Mine Warfare (DOD) The strategic, operational, and tactical use of mines and mine countermeasures. Mine warfare is divided into two basic subdivisions: the laying of mines to degrade the enemy's capabilities to wage land, air, and maritime warfare;

[14] These definitions were listed in Joint Publication 1-02 as amended through April 2010.

and the countering of enemy-laid mines to permit friendly maneuver or use of selected land or sea areas.

Multinational Warfare (DOD) Warfare conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance.

Naval Coastal Warfare (DOD) Coastal sea control, harbor defense, and port security, executed both in coastal areas outside the United States in support of national policy and in the United States as part of this Nation's defense.

Naval Expeditionary Warfare (DOD) Military operations mounted from the sea, usually on short notice, consisting of forward deployed, or rapidly deployable, self-sustaining naval forces tailored to achieve a clearly stated objective.

Naval Special Warfare (DOD) A designated naval warfare specialty that conducts operations in the coastal, riverine, and maritime environments. Naval special warfare emphasizes small, flexible, mobile units operating under, on, and from the sea. These operations are characterized by stealth, speed, and precise, violent application of force.

Nuclear Warfare (DOD, NATO) Warfare involving the employment of nuclear weapons.

Partisan Warfare (DOD, NATO) Not to be used. See guerrilla warfare.

Surface Warfare (DOD) That portion of maritime warfare in which operations are conducted to destroy or neutralize enemy naval surface forces and merchant vessels.

Unconventional Warfare (DOD) A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted through, with, or by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes, but is not limited to, guerrilla warfare, subversion, sabotage, intelligence activities, and unconventional assisted recovery.

Under Sea Warfare (DOD) Operations conducted to establish and maintain control of the underwater environment by denying an opposing force the effective use of underwater systems and weapons. It includes offensive and defensive submarine, antisubmarine, and mine warfare operations.

Enclosure II: Comments from the Department of Defense



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
2500 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2500

SPECIAL OPERATIONS/
LOW-INTENSITY CONFLICT
& INTERDEPENDENT CAPABILITIES

September 1, 2010

FOR: DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, US GOVERNMENT ACCOUNTABILITY OFFICE

SUBJECT: Hybrid Warfare (GAO Engagement 351444)

This is the Department of Defense (DoD) response to the GAO draft report, GAO-10-1036R, 'Hybrid Warfare,' dated August 24, 2010 (GAO Code 351444). As the primary action office, OASD SO/LIC & IC (SOCT) has reviewed GAO's findings and conclusions. Following consultation with the appropriate DoD equities, we concur with the information presented in the report. My point of contact is Ms. Elizabeth Nathan at 703-697-2945.

James Q. Roberts

Principal Director for Special
Operations & Combating Terrorism

(351444)

DOCUMENT NO. 4

SOF (SPECIAL OPERATIONS FORCES) SUPPORT TO POLITICAL WARFARE

UNITED STATES ARMY
SPECIAL OPERATIONS COMMAND

White Paper

Final

10 March 2015

1. Introduction

1-1 Purpose

This white paper presents the concept of SOF Support to Political Warfare to leaders and policymakers as a dynamic means of achieving national security goals and objectives. Embracing the whole-of-government framework with significant targeted military contributions, Political Warfare enables America's leaders to undertake proactive strategic initiatives to shape environments, preempt conflicts, and significantly degrade adversaries' hybrid and asymmetric advantages.

Applied at the regional or global level, Political Warfare emerges from a persistent and purposeful synergy of diplomatic, economic, informational, and military efforts in unified campaigns where military contributions support the attainment of broader strategic end states. Taking advantage of skills, methods, and approaches resident in Special Operations Forces (SOF), Political Warfare's military aspects integrate counter-unconventional warfare (C-UW) and unconventional warfare (UW), foreign internal defense (FID), Security Sector Assistance (SSA), and Information and Influence Activities (IIA), closely calibrated with and in support of those of other government departments.

Political Warfare is a strategy suited to achieve U.S. national objectives through reduced visibility in the international geo-political environment, without committing large military forces. Likewise, Political Warfare can function as a critical, integrating element of U.S. national power against non-state adversaries such as the current Islamic State in Iraq and the Levant (ISIL). Most often, the Department of Defense role in Political Warfare will be one of supporting other U.S. Government agencies that are more likely to lead strategy and planning development.

1-2. Background

Political Warfare emerges from the premise that rather than a binary opposition between "war" and "peace," the conduct of international relations is characterized by continuously evolving combinations of collaboration, conciliation, confrontation, and conflict. As such, during times of interstate "peace," the U.S. government must still confront adversaries aggressively and conclusively through all means of national power. When those adversaries practice a form of Hybrid Warfare employing political, military, economic, and criminal tools below the threshold of conventional warfare, the U.S. must overmatch adversary efforts—though without large-scale, extended military operations that may be fiscally unsustainable and diplomatically costly. Hence, the U.S. must embrace a form of sustainable "warfare" rather than "war," through a strategy that closely integrates targeted political, economic, informational, and military initiatives in close collaboration with international partners. Serving the goals of international stability and interstate peace, this strategy amounts to "Political Warfare."

As will be described here, Political Warfare encompasses a spectrum of activities associated with diplomatic and economic engagement, Security Sector Assistance (SSA), novel forms of Unconventional Warfare (UW), and Information and Influence Activities (IIA). Their related activities, programs, and campaigns are woven together into a whole-of-government framework for comprehensive effect. In this regard, Support to Political Warfare is a novel concept in comparison to the last generation of national security thinking and military operational concepts. Yet, Political Warfare is not without recent precursors in U.S. policy and strategy, with the Cold War being a prime example of approaches foreshadowing the current conception.

a. The Twentieth-Century Normal: Cold War and Political Warfare

From our perspective today, the great twentieth-century struggle against communism appears quite different from the current condition. During the Cold War, "winning" was defined as a broad approach to limit, diminish or defeat Communism. No comparable definition of "winning" exists today, as the U.S. struggles to integrate responses to crises as diverse as Ukraine, ISIL, Iranian nuclearization, African Islamist militancy, and even Ebola into a coherent strategy. Additionally, a massive defense infrastructure and budget to support technologically advanced and highly destructive weapons systems were considered integral to anti-Soviet strategy—to the point that the size of the arsenal and accompanying budget was used to signal U.S. prioritization of containing and rolling back communism. Likewise, the U.S. leadership periodically prosecuted large-scale, sustained conventional campaigns along the margins of the communist world—Korea, and Vietnam are examples of these, as was the basing and reinforcement of U.S. forces in Central Europe.

Considered from another perspective, Cold War policies foreshadow the proposed concept of political warfare. During the cold War era, the West's political and military leadership knew well that the ultimate center of gravity consisted of the cognitive and affective fields of the Human Domain. Additionally, while prior to WWII American military operations were frequently unintegrated with efforts of other U.S. Government (USG) organizations addressing related strategic issues, during that conflict and the Cold War the anti-Communist mission became a unified objective across

the federal government. This can be seen in the political-diplomatic-ideological goals of the Marshall Plan, the aspirations of the Truman Doctrine, and particularly the political and socio-cultural effect sought from the establishment of NATO and the myriad of overt and covert initiatives in the cognitive and affective realms of the Human Domain both east and west of the Iron Curtain.[1]

Finally, though the U.S. employed military force in foreign areas in an overwhelmingly reactive fashion up through the Korean War, subsequent military engagement was frequently preemptive, with associated paramilitary and intelligence activities being proactive. As an example, Cold War counter-insurgency (COIN) and UW activities in Southeast Asia and several Central and South American countries, generally conducted by Special Operations Forces (SOF)—were pre-emptive, seeking to limit the spread of global Communism.

Beyond the levels of policy and operations, the very conceptual basis and rationale for U.S. concepts of Political Warfare were articulated during the early Cold War years by George F. Kennan, America's foremost Soviet expert and State Department architect of the policy of Containment of Soviet/communist expansion. In 1948, Kennan called for "the logical application of Clausewitz's doctrine in time of peace." While stopping short of the direct kinetic confrontation between two countries' armed forces, "political warfare is the employment of all the means at a nation's command . . . to achieve its national objectives." A country embracing Political Warfare conducts "both overt and covert" operations in the absence of declared war or overt force-on-force hostilities. Efforts "range from such overt actions as political alliances, economic measures…, and 'white' propaganda to such covert operations as clandestine support of 'friendly' foreign elements, 'black' psychological warfare and even encouragement of underground resistance in hostile states."

Recognizing that other world powers such as the British Empire's Political Warfare Executive and the Soviet Union regularly practiced Political Warfare, Kennan called for America's post-WWII leadership to disabuse itself of the "handicap" of the "concept of a basic difference between peace and war," and wake up to "the realities of international relations—the perpetual rhythm of struggle, in and out of war."[2] To match this rhythm, Kennan in effect called for the broad use of UW, one of the primary mission areas of Special Forces in the 1950s.

b. The Post-Cold War Retreat from Political Warfare

Therefore, on the levels of policy, strategic thought and operations, approaches foreshadowing Political Warfare have not been alien to American national security system. Rather, it can be argued that the U.S. has "gotten out of the habit of waging political warfare since the end of the Cold War." With a residual preference for large-scale combined arms operations reminiscent of Operation Desert Storm, the U.S. entered the

[1] Peter Finn and Petra Couvee, *The Zhivago Affair: The Kremlin, the CIA, and the Battle over a Forbidden Book* (New York: Pantheon, 2014); Martin Vennard, "How the CIA Secretly Published Dr Zhivago," BBC World Service, 23 June 2014: http://www.bbc.com/news/magazine-27942646.

[2] George Kennan, "Policy Planning Memorandum," May 4, 1948, National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2, accessed June 9, 2014 http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

post-September 11, 2001 world with a reliance on "public diplomacy aimed at 'telling America's story,'"[3] in order to diffuse anti-American animus in the Muslim world. Likewise, military responses to post-9/11 challenges emerged as sustained, large scale deployments to Iraq and Afghanistan, in addition to frequently reactive counterterrorism (CT) and COIN.

Given the emerging threat environment, however, as well as the prohibitively costly and politically unsustainable nature of most kinds of extended, large scale military operations, the time has come for Political Warfare to recapture a predominant position in U.S. national security policy and execution. With innovative state and nonstate adversaries willing to confront the U.S. across a spectrum of sustained activities, American leaders can avoid the conceptual "handicap" highlighted by Kennan, and embrace ongoing Political Warfare, to include the informational, influence, and unconventional warfare campaigns to which Kennan pointed. Of course, these kinds of activities require miniscule resources when compared to the Cold War and operations in Iraq and Afghanistan, and are the very kinds of campaigns at which SOF excels.

1-3. Emerging Operating Environment

The operating environment that has emerged since the end of the Cold War has also demonstrated the intellectual and policy futility of a dichotomous understanding of war and peace and of traditional understandings of military-dominated, openly declared, force-on-force armed confrontation as the predominant mode of warfare. Rather, resurgent state adversaries, rising regional powers, and nonstate armed elements seeking to dominate the military, political, and ideological arenas have practiced novel forms of warfare during times of both "peace" and "war." The U.S. will not be able to counter such threats and seize the strategic initiative without a more agile employment of whole-of-government resources, driven by a more supple national security sensibility embracing Political Warfare.

a. Hybrid Warfare: Russia in its 'Near Abroad'

The most immediately visible form of novel warfare practices during "peacetime" can be seen in Russia, the inheritors of what Kennan referred to as "the most refined and effective" conduct of Political Warfare "of any in history."[4] Since the early spring of 2014, Russia's form of Political Warfare has emerged as intensive Hybrid Warfare in Ukraine. Russia currently employs special operations forces, intelligence agents, political provocateurs, and media representatives, as well as transnational criminal elements in eastern and southern Ukraine.[5] Resourced and orchestrated by the Kremlin and operating with

[3] Max Boot, Jeane J. Kirkpatrick, Michael Doran, and Roger Hertog, "Political Warfare," Policy Innovation Memorandum No. 33, Council on Foreign Relations, June 2013, accessed May 16, 2014, http://www.cfr.org/wars-and-warfare/political-warfare/p30894.

[4] George Kennan, "Policy Planning Memorandum," May 4, 1948, National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2, accessed June 9, 2014 http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

[5] John Kerry, Secretary of State, Opening Statement Before the Senate Committee on Foreign Relations, *National Security and Foreign Policy Priorities in the FY 2015 International Affairs Budget*, 113th Cong., 2d sess., April 8, 2014; see also Victoria Nuland, Assistant Secretary, Bureau of European and Eurasian Affairs, Statement Before the Senate Committee on Foreign Relations, *Ukraine: Countering Russian Intervention and Supporting Democratic State*, 113th Cong., 2d sess., May 6, 2014.

differing degrees of deniability or even acknowledgement, Russian Hybrid Warfare uses such "little green men" for classic UW objectives. These objectives include causing chaos and disrupting civil order, while seeking to provoke excessive responses by the state's security organs, thus delegitimizing the Kiev government. Additionally, Russian elements have organized pro-Russian separatists, filling out their ranks with advisors and fighters. Russia's UW has also included funding, arming, tactical coordination, and fire support for separatist operations.[6] The latter component, combined with large-scale conventional force posturing along the Russian-Ukrainian border, aerial harassment of NATO naval assets in the Black Sea, and continuous diplomatic engagement and intimidation of NATO states and the Ukraine government, illustrate the Kremlin's embedding of UW in a much broader Hybrid Warfare campaign.

While enabling a frequency of tactical success against Ukrainian forces putting the latter at a distinct strategic disadvantage, insurgency aided by Russian UW has achieved operational goals of gaining local supporters and intimidating dissenters into acquiescing to a separation from the government in Kiev.[7] In such fashion, Russian Hybrid Warfare has secured the strategic goals of acquiring the Crimea, pushing the pro-Russian buffer zone farther west into the Ukraine, threatening Odessa, and increasing the perception of Russian power in Azerbaijan and Armenia,[8] as well as in the Asia-Pacific region, in the latter case to the potential detriment of U.S. energy policy interests.[9]

Russian operations in Ukraine are part of a broader Hybrid Warfare offensive over the past decade. Associated actions have included cyber-attacks on private and government websites in former Soviet areas—to include NATO member states; agitation and economic infiltration among Russian speaking populations in the Baltics; and support to separatists in former Soviet Republics in order to provoke disproportionate local responses that could justify Russian conventional invasion—the case in Georgia. Likewise, Russian Hybrid Warfare has used oil and natural gas exports as a tool to influence government policies in former Soviet and central Europe; prosecuted overall force expansion programs accompanied by conventional force posturing in military exclaves among NATO states; and returned to violations of NATO and NATO-partner countries' airspace and maritime zones, while prosecuting an influence and psychological operations campaign in the Russian-speaking diaspora, at times with the goal of promoting secession from states bordering NATO and affiliation with Russia.[10]

---

[6] Victoria Nuland, Assistant Secretary, Bureau of European and Eurasian Affairs, Statement Before the Senate Committee on Foreign Relations, *Ukraine: Countering Russian Intervention and Supporting Democratic State*, 113th Cong., 2d sess., May 6, 2014.

[7] John Kerry, Secretary of State, Opening Statement Before the Senate Committee on Foreign Relations, *National Security and Foreign Policy Priorities in the FY 2015 International Affairs Budget*, 113th Cong., 2d sess., April 8, 2014.

[8] "Amid Karabakh Tensions, Both Armenia and Azerbaijan View Russia Uneasily," *Radio Free Europe/Radio Liberty*, 13 Aug 2014: http://www.rferl.org/content/nagorno-karabakh-azerbaijan-armenia-wary-russia/26528994.html; Brenda Shaffer, "Russia's Next Land Grab," *New York Times*, Sept 9, 2004: http://www.nytimes.com/2014/09/10/opinion/russias-next-land-grab.html?_r=0.

[9] James Paton and Rebecca Penty, "Russia-China Gas Accord to Pressure LNG in Canada, Australia," *Bloomberg News*, 11 Nov 2014: http://www.bloomberg.com/news/2014-11-11/russia-china-natural-gas-ties-seen-leading-to-lng-project-delays.html.

[10] Russia to Put Kaliningrad Missile Defense Radar on Full Combat Duty in December," Sputnik News.com, 15 Oct 2014: "http://www.sputniknews.com/military/20141015/194122624/Russia-to-Put-Kaliningrad-Missile-Defense-Radar-on-Full-Combat.html; "Kaliningrad: European fears over Russian missiles," BBC News, 16 Dec 2013: http://www.bbc.com/news/world-europe-25407284; Nikolas K. Gvosdev, "The Bear

Russian measures in Ukraine and beyond over the past decade illustrate the implementation of emerging Russian operational concepts. Russian military theoreticians have argued for a "combination of political, economic, information, technological, and ecological campaigns in the form of indirect actions and nonmilitary measures" in order to "level off the enemy's superiority in armed struggle . . . neutraliz[ing] adversary actions without resorting to weapons.[11] In 2013, the Russian Chief of the General Staff noted that "the role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness." These means include "special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."[12] Significantly, with the exception of the Georgian conflict, these concepts and their implementation in the past few years stop short of war itself, and are taken in order to obtain political-economic benefit. Hence, Russian Hybrid Warfare has many elements of what the U.S. considers Political Warfare.[13]

b. China's Unrestricted Warfare

Even during the period of post-Soviet Russian weakness prior to Vladimir Putin's ascent, other countries were developing concepts specifically designed to counter the U.S. conventional superiority. In 1999, two Chinese People's Liberation Army colonels argued that in order to counter the conventional superiority of the U.S., China should use a host of methods, many of which lie out of the realm of conventional warfare. These methods include trade warfare, financial warfare, ecological warfare, psychological warfare, smuggling warfare, media warfare, drug warfare, network warfare, technological warfare, fabrication warfare, resources warfare, economic aid warfare, cultural warfare, and international law warfare.[14] These methods amount to "unrestricted warfare," whose first rule stipulates "that there are no rules, with nothing forbidden."[15]

In 2003, the Chinese Communist Party Central Committee and the Central Military Commission drew on "unrestricted warfare" concepts to promulgate a "Three Warfares" concept. Here, *Psychological Warfare* seeks to undermine an enemy's operational ability by demoralizing enemy military and civilian populations through "television, radio

Awakens: Russia's Military Is Back," *The National Interest*, November 12, 2014: http://nationalinterest.org/commentary/russias-military-back-9181

[11] Col. S.G. Chekinov (Res and Lt. Gen. S.A. Bogdanov(Ret.), "The Nature and Content of a New-Generation War," *Military Thought: A Russian Journal of Military Theory and Strategy*, No. 4, 2013, 16: http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf.

[12] Dr Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," July 2014: https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/#more-2291.

[13] Also see United Kingdom Parliament, Defence Committee, Third Report – "Towards the Next Defence and Security Review: Part Two NATO," 22 July 2014: http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/358/35805.htm#a4.

[14] Bill Gertz, *The China Threat: How the People's Republic Targets America* (Washington, D.C.: Regnery Publishing, 2000), 16.

[15] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, trans. Foreign Broadcast Information Service. (Beijing: PLA Literature and Arts Publishing House, 1999) 2.

broadcast, loudspeakers, leaflets, and calculated military operations,"[16] accompanied by "diplomatic pressure, rumors, false narratives, and harassment to 'express displeasure, assert hegemony, and convey threats."[17] *Media Warfare* seeks to influence domestic and international public opinion to build support for military actions and dissuade adversaries from actions contrary to China's interests. It also targets the Chinese diaspora to garner support for "Chinese public diplomacy and espionage operations throughout the world."[18] *Legal Warfare* uses international and domestic law to claim the legal high ground or assert Chinese interests. It can be employed to hamstring an adversary's operational freedom and shape the operational space. Legal warfare is also intended "to build international support and manage possible political repercussions of China's military actions."[19] China has already used Legal Warfare to cause friction among adversaries and influence interpretation of international law.

c. Iranian Asymmetric Warfare

Iran is distinct from Russia and China. Nevertheless, it practices a mode of continual warfare indicative of the emerging and future operating environments characterized by asymmetry, the pursuit of political goals, and the avoidance of large-scale conflict. Conceived by its developers as defensive, Iran's military doctrine combines the use of conventional, guerrilla, and special operations forces, in order to "deter an attack, survive an initial strike, retaliate against an aggressor, and force a diplomatic solution to hostilities while avoiding any concessions that challenge its core interests."[20] While fielding more capable ballistic missiles to counter threats from Israel and other actors in the region and developing the capability to launch intercontinental ballistic missiles,[21] Iran has sought anti-access and area denial capabilities through asymmetric means, to include "hit and run attacks with sea and land-launched anti-ship cruise missiles, mines, mini-subs and suicide boats,"[22] as well as cheaply-produced fast attack craft amounting to little more than speed boats—able to endanger much more expensive and slow moving U.S. vessels.[23]

A major element of Iranian asymmetric warfare involves covert support to proxy forces in the region and beyond, whose activities support Iranian national objectives. The

[16] Timothy A. Walton, "China's Three Warfares," Special Report 3, Delex Systems, January 18, 2012, 5, accessed July 30, 2014, http://www.delex.com/data/files/Three%20Warfares.pdf.

[17] Department of Defense China Report May 2013 quoted in Bill Gertz, "Warfare Three Ways: China Waging 'Three Warfares' against United States in Asia, Pentagon Says," The Washington Free Beacon, March 26, 2014: http://freebeacon.com/national-security/warfare-three-ways/.

[18] Timothy A. Walton, "China's Three Warfares."

[19] Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011," August 2011, 26, accessed August 1, 2014: http://www.defense.gov/pubs/pdfs/2011_cmpr_final.pdf.

[20] Department of Defense, "Annual Report on Military Power of Iran," Executive Summary, January 2014, accessed August 11, 2014, http://freebeacon.com/wp-content/uploads/2014/07/Iranmilitary.pdf.

[21] Department of Defense, "Annual Report on Military Power of Iran," Executive Summary, January 2014, accessed August 11, 2014, http://freebeacon.com/wp-content/uploads/2014/07/Iranmilitary.pdf

[22] Michael Cummings and Eric Cummings, "The Cost of War with Iran: An Intelligence Preparation of the Battlefield," *Small Wars Journal*, August 31 2012, accessed August 20, 2014, http://smallwarsjournal.com/jrnl/art/the-costs-of-war-with-iran-an-intelligence-preparation-of-the-battlefield.

[23] Barbara Starr, "Official: U.S. Vessels Harassed by High-Speed Iranian Boats," CNN, January 13, 2012, accessed August 20, 2014, http://www.cnn.com/2012/01/13/us/iran-boats-tensions/.

Iranian Revolutionary Guards Corps (IRGC) is funded through an annual military budget of $5 billion as well as through funds based on widespread legal and illicit economic enterprises estimated at $13 billion per year.[24] The IRGC provides material support to terrorist or militant groups whose goals are broadly aligned with Iranian interests—including countering U.S. regional engagement. These include HAMAS, Lebanese Hezbollah, the Palestinian Islamic Jihad, the Taliban, and Iraqi Shia groups.[25] The IRGC has also enabled targeted execution operations in the U.S. and European capitals.

Along with the UW mission of support to proxy forces, IRGC and other regime-affiliated elements have provided funding to Shiite educational initiatives and political dissident groups in the Arab Gulf region, and have perpetuated an influence campaign seeking to discredit regional rulers on religio-ethical grounds.

Finally, Iran has rapidly developed its defensive and offensive cyber capabilities. Part of this effort seeks to keep Iranians from encountering Western ideas and content, which would contribute to the development of a "soft revolution" that would harm the stability of the regime.[26] Iranian asymmetric warfare is thus directed against domestic, regional, and global perceived threats, and clearly mobilizes resources beyond the traditional military sector.

d. Hezbollah

As one of Iran's chief proxies, Hezbollah has employed multiple lines of effort in conducting asymmetric political warfare, directed against Israel, domestic political opponents, and the interests of adversary foreign states operating in Lebanon. In addition to widespread and persistent use of terrorism against targets in Lebanon, the Middle East, and Europe as well as the western hemisphere, Hezbollah has also employed insurgency tactics, rendering parts of Lebanese territory as a sort of "Hezbollah-land" passable by government forces only at the former's discretion. Inspired by its Iranian patron, Hezbollah has also engaged in Counter-UW (C-UW) in Syria, shoring up the forces of the Assad regime. Hezbollah has prosecuted a sophisticated influence campaign within its area of control by using terrestrial and satellite television, radio, and web-based media, in addition to powerfully emotive images and messages on billboards, and even in museums. Through Iranian funding, as well as organized crime, extortion, and narco-trafficking in the region and as far afield as Latin America, it has also been able to sustain social welfare institutions gaining adherents in and beyond the Shiite community, gaining legitimacy for itself while discrediting the Lebanese state. At the same time, it has used its communal and regional support base to participate and gain predominance in Lebanon's political institutions, further influencing the country's geopolitical orientation. All the while, Hezbollah has gained much increased sophistication

[24] Michael Rubin, "U.S. Response to Iran's Use of Unconventional Warfare" (PowerPoint presentation at USASOC Irregular Warfare Seminar, Fort Bragg, NC, August 28, 2014). Mr. Rubin also highlighted the IRGC's involvement in the Iranian electronics industries such as computers, telephones, scanners, and SIM cards; the IRGC has signed $50 billion worth of contracts with the Oil Ministry under President Ahmadinejad; the IRGC operates the cargo airport Payam International Airport; and has 25 gates outside customs control at the Imam Khomeini International Airport.

[25] Department of Defense, "Annual Report on Military Power of Iran," Executive Summary, April 2012, accessed August 11, 2014, http://fas.org/man/eprint/dod-iran.pdf.

[26] Gabi Siboni and Sami Kronenfeld, "Developments in Iranian Cyber Warfare, 2013-2014," *INSS Insight* No. 536, April 3 2014, accessed August 20, 2014, http://www.inss.org.il/index.aspx?id=4538&articleid=6809.

in the technical, tactical, and operational components of warfighting—synchronizing military operations to clear political end states.

2. Future Operating Environment

a. Global Power Diffusion

The U.S. National Intelligence Council (NIC) currently projects a much greater diffusion of global power in the near future, with the resultant multipolarity driving geopolitical instability. According to the NIC, "by 2030, no country—whether the U.S., China, or any other large country—will be a hegemonic power."[27] Rising regional states such as China, Russia, India, Brazil, Indonesia, Turkey and Iran will assert growing power and influence regionally and globally to secure their political, social, or economic interests. The U.S. national leadership will thus employ the elements of national power in an international environment where alliances change more frequently and adversarial relationships will be more common and nuanced than in the past.

b. Non-State and Semi-State Actors

The diffusion of global power will also be manifest as an increased role by non-state actors seeking greater influence from the local-to-global level. The rapid spread of ever-improving weapons and information technology will prove an enabler in this respect: "Individuals and small groups will have greater access to lethal and disruptive technologies (particularly precision-strike capabilities, cyber instruments, and bioterror weaponry), enabling them to perpetrate large-scale violence—a capability formerly the monopoly of states."[28] Violent extremists as well as criminal organizations will use these tools with little restraint in order to achieve their desired effects. Indeed, the cyber domain in particular will permit small groups and individuals to achieve truly disproportionate effects.

Notably, however, recent events suggest that nonstate actors may increasingly aspire towards para-statal manifestations. Foreshadowed by the Palestine Liberation Organization on the political-economic pane during the 1970s and 1980s, groups like Hamas and Hezbollah have not only sought not to oppose internal and external powers, but they have sought to act like a state, or usurp the state itself.[29] Most recently, Sunni Jihadi extremists claiming a boundless "Islamic State" now seek to overthrow national governments, local administrations, and social-political structures in a wide swathe from eastern Syria to northwestern Iraq, replacing them with a regional Muslim Caliphate obtaining funds from nonstate sponsors in the very Arab Gulf states whose governments are now cooperating with the U.S.[30] In a more geographically focused way,

[27] National Intelligence Council, *Global Trends 2030: Alternative Worlds*, 18.

[28] National Intelligence Council, *Global Trends 2030: Alternative Worlds*, iii.

[29] For "parastatal," see Yezid Sayigh, *Armed Struggle and the Search for State: The Palestinian National Movement, 1949–1993* (Washington, D.C.: Institute for Palestine Studies, and Oxford: Clarendon Press, 1997)

[30] The Islamic State is also known as the Islamic State in Iraq and Syria (ISIS) and Islamic State of Iraq and the Levant (ISIL). See Matthew Levitt, "Terrorist financing and the Islamic State," Congressional Testimony Presented before the House Financial Services Committee, Nov 13, 2014: http://www.washingtoninstitute.org/policy-analysis/view/terrorist-financing-and-the-islamic-state; Dennis Ross, "A Strategy for Beating the Islamic State," *Politico*, September 2, 2014: http://www.washingtoninstitute.

the Houthi rebels have of late solidified their hold on a quasi-state in Northwestern Yemen, and moved beyond their traditional stronghold and preference for autonomy from the central government, to occupy the country's Red Sea Ports and parts of the capitol.[31] These cases have also featured evolving combinations of insurgency, acts of terrorism, and UW aided by information campaigns, political alliance-making, and economic measures—in effect kinetic action along with Political Warfare.

c. Advancing Computing Power and Information and Communications Technologies

Technology will continue to influence the course, tempo, and toll of conflict in the FOE, particularly through advances in computing power and the broadening dissemination of information communications technologies (ICT). Regarding the former, today's computer systems process a much greater number of more complicated operations than in the recent past; processing speed and complexity advance at a staggering rate. These increases in speed and operational complexity will characterize consumer products such as laptops and tablet computers. Significantly, this class of devices will also be available more widely in the FOE, at lower prices. Therefore, a technology once the preserve of governments, prestigious labs, and the wealthy will be accessed by a broadening social stratum—to include those in areas characterized by increased population, urbanization, climate degradation and non-state actor proliferation.

Beyond computing power, the truly revolutionary aspect of emergent technology development is in the realm of communications, which has seen the rapid diffusion of both person-to-person and social media ICTs. Cellular, Wi-Fi, and ground-based networks can move such large amounts of information so much farther and faster than in the recent past as to permit a speed of communication and action quite outpacing even a decade ago. Global internet penetration rates, as well as the rate by which mobile access of the internet increases, continue to increase.[32] Further, the tools associated with such networks have become increasingly inexpensive, disposable, and broadly capable. Thus, the network-creating nature of social media will ensure that individual or small group experiences in the FOE become shared consciousness of a transnational and self-selecting collective.

An ease of message making and dissemination will thus characterize the FOE, accelerating a "battle of narratives" in which nonstate elements and amorphous, event-driven groupings will erase the relative nation-state monopoly of narratives during the

org/policy-analysis/view/a-strategy-for-beating-the-islamic-state; Jean-Pierre Filiu, James F. Jeffrey, Michael Eisenstadt, "Defeating ISIS, from Strategy to Implementation," Washington Institute Policy Watch 2315, September 23, 2014: http://www.washingtoninstitute.org/policy-analysis/view/defeating-isis-from-strategy-to-execution.

[31] David Hearst, "Blowback in Yemen: Houthi advance is a Saudi nightmare," *Middle East Monitor*, 21 October 2014: https://www.middleeastmonitor.com/articles/middle-east/14785-blowback-in-yemen-houthi-advance-is-a-saudi-nightmare.

[32] "Social Networking Reaches Nearly One in Four Around the World, Emarketeer.*com*, Jun 18, 2013: http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976; Amit Misra, "Social Media Growth 2013 – 2017: Every Forth Person On Planet Use Social Media [STUDY]," Dazeinfo.com, June 20, 2013: http://www.dazeinfo.com/2013/06/20/social-media-growth-2013-2017-every-forth-person-on-planet-use-social-media-study/.

industrial era.[33] Thus the diversity of narratives, their speed of dissemination, and their rate of change will be dizzying, to the advantage of all but state actors. As such, the FOE will complete the transition of the internet from being a mostly passive canvas of material (Web 1.0) to an environment where users are contributors through wikis, blogs, and social networking (Web 2.0), and then to one where computers regularly manipulate data for purposes of analysis, profiling, and influence (Web 3.0). The potential for ethically unconstrained adversary states and non-states to employ these technologies to Hybrid Warfare advantage will remain great.

d. Hybrid Warfare

As we saw with the Russian case above, hybrid threats will likely define the nature of warfare in the future operating environment, providing a diverse array of options through which America's adversaries will confront us and our global partners. Hybrid Warfare includes "any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain their political objectives." Hybrid threats will also liberally employ proxies, surrogates, and unwitting population groups, as well as actions whose first-order effects are non-violent. Hoffman describes these effects as "economic and financial acts, subversive political acts like creating or covertly exploiting trade unions and NGOs as fronts, or information operations using false websites and planted newspaper articles," in addition to "diplomatic tools . . . as part of a larger conception of warfare."[34]

Given adversary practices in the emerging operating environment, as well as the likely features of the future operating environment, the U.S. must now develop and implement military operating concepts galvanizing a whole-of-government strategy to contain, and deter threats to our national interests while permitting our national leadership to seize the initiative in international affairs in defense of the American people—yet without major military confrontations and unsustainable budget expenditures. Persistent engagement of Political Warfare, facilitated and synchronized by capabilities inherent to SOF, provides a principal solution set.

3. Military Problem and Components of Solution

3-1 Problem Statement

How does the United States counter and deter the asymmetric and hybrid warfare employed by our state and nonstate adversaries during both "war" and "peace" across

[33] See USJFCOM, The Joint Operating Environment [JOE] (2010); US Army TRADOC, *Operational Environments to 2028: The Strategic Environment for Unified Land Operations*, August 2012: http://www.arcic.army.mil/app_Documents/TRADOC_Paper_Operational-Environments-to-2028-Strategic-Environment-for-Unified-Land-Operations_AUG2012.pdf.

[34] Frank Hoffman, "On not-So-New Warfare: Political Warfare vs. Hybrid Threats," *War on the Rocks*, July 28, 2014:http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/; Mark Lander and Michael R. Gordon, "NATO Chief Warns of Duplicity by Putin on Ukraine," *New York Times*, July 8, 2014: http://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html?_r=0; Frank G. Hoffman, "Hybrid vs. Compound War, The Janus Choice: Defining Today's Multifaceted Conflict," *Armed Forces Journal*, October 2009: http://www.armedforces-journal.com/2009/10/4198658/; Dr. Russell W. Glenn, "Thoughts on Hybrid Conflict," *Small Wars Journal*, 2009: http://smallwarsjournal.com/blog/journal/docs-temp/188-glenn.pdf.

the spectrum of conflict? How can the U.S. respond optimally to hybrid and asymmetric challenges while accounting for fiscal limitations and political sensitivity to large-scale operations? What is the best means to fully synchronize Joint, Interagency, Intergovernmental, and Multinational (JIIM) responses to hybrid challenges?

3-2. Central Idea

U.S. policy makers require a suite of complementary options enabling them to counter and deter hybrid and asymmetric warfare practiced by state and nonstate adversaries. As hybrid and asymmetric warfare rely on surrogates, proxy forces, insurgents and supporting influence operations, effective U.S. policy responses require capabilities to a) comprehensively mitigate the effect of subversion, UW, and delegitimizing narratives in partner countries targeted by adversaries; and b) dissuade adversaries from conducting hybrid warfare by increasing the cost of such activities to the point that they become unsustainable. The former effort involves strengthening the capabilities, capacity, and legitimacy of partners, while the latter involves aggressively countering subversion and UW waged against friendly states, proactively employing coercive diplomacy, legal-economic measures, and UW against adversaries, and aggressively prosecuting a battle of narratives to undermine adversary legitimacy among critical populations.

The U.S. and its partners can indeed overmatch adversaries practicing hybrid warfare and achieve escalation dominance against future adversaries—but only through a thoroughly whole-of-government approach informed by unity of effort and purpose expressed through integrated strategy and cohesive policy options. This all amounts to Political Warfare, a supple, synergistic, and evolving use of "both overt and covert" tools at America's disposal, with an emphasis on coercive diplomatic and economic engagement, Security Sector Assistance (SSA), information and influence activities (IIA), and diverse forms of unconventional warfare (UW).

A thoroughly whole-of-government endeavor, Political Warfare is by no means the preserve of SOF. Given its diplomatic and economic content and its focus on achieving political ends, Political Warfare is likely best led by agencies beyond DoD.[35] Indeed, Political Warfare can only succeed if it is conducted in a way to "elevate civilian power alongside military power as equal pillars of U.S. foreign policy."[36] Yet, as SSA, UW and IIA hinge on skill sets cultivated by SOF, the latter are uniquely positioned to support both the joint force and America's agencies beyond DOD leading Political Warfare strategies. Furthermore, SOF are unique in the Department of Defense, suited to integrate Political Warfare's activities across the JIIM spectrum. Army Special Operators have a proven track record of bridging indigenous forces, local populations, Joint Force components, U.S. agencies, and coalition partners needed for an effective Political Warfare response to hybrid warfare. SOF must be the expert practitioners of this form of warfare to lead DOD's contribution.

[35] See this discussion in the State Department context nearly a decade ago: Dave Kilcullen, "New Paradigms for 21st Century Conflict," *State Department eJournal*, June 2007, found at http://smallwarsjournal.com/blog/new-paradigms-for-21st-century-conflict.

[36] Department of State & USAID, *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review* (Washington, DC: 2010), Executive Summary, 2: http://www.state.gov/documents/organization/153635.pdf.

3-3. Definitional Building Blocks of 21st-Century Political Warfare

Political Warfare emerges from a Whole-of-Government approach to international diplomatic and security engagement, with agencies beyond DOD performing critical, if not leadership, roles. The overall Political Warfare effort relies on the synchronized and evolving combination of capabilities possessed, enabled, or supported by SOF. They include coercive diplomacy, economic coercion and engagement, Security Sector Assistance, Unconventional Warfare, and information and Influence Activities. Understanding these capabilities is thus integral to generating a concept of Political Warfare appropriate to the future operating environment.

a. Diplomacy: Persuasive and Coercive

Diplomacy, and its economic means, is an important initial tool through which to counter adversary hybrid warfare against partner states, and is often critical to setting the conditions for more aggressive economic or military responses. One form of diplomacy may be referred to as *persuasive* diplomacy. Other options include the employment of unconventional diplomacy or unconventional statecraft.[37] Here U.S. diplomacy can incline friends and neutral states to more robust participation in countering adversary hybrid warfare. In persuasive diplomacy, the U.S. can work bilaterally as well as multilaterally. Addressing partner or potential partner countries, the U.S. may establish bilateral strategic agreements in the realms of security, economics, and areas of particular concern to the particular country, bolstered by aid targeted to areas that implicitly support common Political Warfare efforts. Likewise, the U.S. can indicate diplomatic favor and increase the regional standing of the state in question through frequent cabinet level visits and summits, as well as through the kind of cultural exchanges and ties used so well during the Cold War to increase mutual bilateral awareness and sympathy.

Further, the American diplomacy can advocate for partner state leadership roles in regional organizations—African Union, European Union, etc.—as well as in global bodies such as the UN and World Bank. Access to leadership roles in such bodies increases the standing of the country in question, enables more meaningful diplomatic cooperation, and empowers both the U.S. and the partnered sate to counter hybrid warfare activities more effectively and with increased international credibility. All these bilateral efforts have the benefit of communicating commitment to the partner state, as well as resolve to the adversary state or nonstate actor(s). These efforts also prepare the environment for subsequent Political Warfare military engagement, enabling the kinds of SOF activities to be described further on in this paper.

At the multilateral level, effective Political Warfare requires that the U.S. continue to engage international organizations persistently and positively, motivating them both to adopt positions and programs counter to the activities associated with adversary hybrid warfare, and to censure those countries engaging in it. Though the processes and at

[37] Schmitt and Wall define unconventional statecraft as "external support by one state to insurgents in another" and unconventional statecraft activities are "designed to coerce, disrupt, or overthrow a government or occupying power by operating with or through a resistance movement or insurgency in a denied area. It can include, inter alia, diplomatic, economic, information, intelligence, or military support and can occur during peacetime or in an ongoing non-international or international armed conflict." Michael N. Schmitt and Andru E. Wall, "The International Law of Unconventional Statecraft," *Harvard National Security Journal*, no. 5 (2014), 352-353.

times outcomes in fora such as the UN, EU, AU, ASEAN, the World Court, INTERPOL, etc., are perhaps suboptimal, they are critical to creating a commonality of attitudes and concerns, for strengthening bilateral relationships, and for providing backbone to neutral or targeted states. Furthermore, engagement with these bodies demonstrates consideration for the concerns of members and for international legality, and may result in decisions that bind member states.

Finally, regional security alliances such as NATO are critical to attaining a consensus on the character and dangers of hybrid warfare, and also to developing diplomatically sustainable political-military-economic response, even if all member states do not act explicitly in terms of Political Warfare. Ultimately, these global bodies—particularly those which integrate regional governments in common security arrangements—play to SOF's strength as JIIM connective tissue for Political Warfare, particularly through the Global SOF Network (GSN), to be discussed further on.[38]

Beyond persuasive diplomacy, the U.S. may apply persistent *coercive* diplomacy to hybrid threats, relying on capabilities which mesh SOF and CF strengths. Coercive diplomacy emerges from theories related to deterrence and compellance developed during the Cold War.[39] Its originator, Alexander George, aimed "to articulate a policy relevant theory of coercive diplomacy in which threats, persuasion, positive inducements, and accommodation were integrated into a crisis bargaining strategy that provided political leaders with an alternative to war or to strictly coercive military strategies."[40] Indeed, the U.S. and NATO sought to contain and roll back Soviet adventurism without the need for large scale, sustained military action. Such action would be considered a total failure. Therefore, coercive diplomacy is thus well-suited to today's political-economic circumstances.

Coercive diplomacy is a "political-diplomatic strategy that aims to influence an adversary's will or incentive structure." Rather than deterrence, which is *preventative* in nature, coercive diplomacy is intended to cause an adversary to *cease* activities, and if possible *reverse* previous actions and change policies.[41] In this respect, excessive use of coercion in the absence of a convincing initial provocation reduces the approach to one of bullying aggression. Rather, the "central task of coercive diplomacy [is] to create in the opponent the expectation of costs of sufficient magnitude to erode his motivation to continue what he is doing," by combining diplomatic, economic, and military threats with broader mobilization of partners and allies, as part of a bargaining strategy including "conditional inducements of a positive character" to incentivize an adversary's retreat from aggressive activities.[42]

[38] "Versatile Special Operations Forces for New Threats," NATO News Room, 22 May 2014: http://www.nato.int/cps/en/natohq/news_111124.htm.

[39] See T. C. Schelling, *Arms and Influence* (New Haven, CT: Yale University, 1966).

[40] Jack S. Levy. "Deterrence and Coercive Diplomacy: The Contributions of Alexander George," Political Psychology 29:4 (2008), 539.

[41] David M. Lampton, "The U.S. and China: Sliding from Engagement to Coercive Diplomacy, PacNet #63, CSIS, Aug 4, 2014: http://csis.org/publication/pacnet-63-us-and-china-sliding-engagement-coercive-diplomacy

[42] Alexander L. George, *Forceful Persuasion: Coercive Diplomacy as an Alternative to War* (Washington, DC: USIP Press, 1991), 10, 11.

Coercive diplomacy is therefore just that—diplomacy providing political leaders an alternative to war. Yet, the strategy does envision the use of force, for demonstrative and psychological effect. Rather than a "quick, decisive military strategy" seeking to destroy enemy capabilities to perpetuate conflict by "bludgeoning him . . . or physically preventing him" from acting in a certain manner,[43] coercive diplomacy advocates for "the limited and selective use of force in discrete and controlled increments,"[44] and "carefully measured, discrete doses."[45] In this conception, force is a "much more flexible, refined, psychological instrument of policy."[46] The "exemplary use of quite limited force" must be of the "appropriate kind to demonstrate resolution to protect one's interests and establish the credibility of one's determination to use more force if necessary."[47] Leaving the adversary "the capacity of organized violence" but driving them to "choose not to use it,"[48] effectively employed coercive diplomacy may "induce an adversary to comply with one's demands . . . while simultaneously managing the crisis to prevent unwanted military escalation."[49]

Coercive diplomacy is open to failure, of course—the need to conduct Operation Desert Storm in 1991 could be considered such failure, as the military and diplomatic coercion of the preceding several months did not compel Saddam Hussein's withdrawal. Likewise, coercive diplomacy has not been employed with effect in the Korean Peninsula, and after the U.S. threatened Japan with an oil embargo in July 1941, "coercive diplomacy provoked the adversary into a decision for war."[50] There have been some notable cases of its success however, to include during the Cuban missile Crisis, and potentially during the 2013 chemical weapons crisis in Syria.[51]

International relations scholars have enumerated several conditions which must obtain in order for coercive diplomacy to be judged a success. Many of these hinge on the adversary leadership's perceptions and goals, as well as fear of escalation. Additionally, experts consider the coercing state's strength of motivation, clarity of goals, sense of urgency and red lines, and domestic political support as critical variables to determining the viability or success of a coercive diplomacy campaign.[52]

While these variables rely on multiple interactive factors, it is in the realm of an additional condition—usable military options—that the Joint Force, and SOF in particular, can empower our national leadership with viable options to conduct coercive diplomacy.

---

[43] Alexander George et al, *The Limits of Coercive Diplomacy*, 2nd Rev. ed. (Boulder, Colorado: Westview Press, 1994), 19.

[44] Jack S. Levy. "Deterrence and Coercive Diplomacy," 539.

[45] Alexander L. George, *Forceful Persuasion*, 43.

[46] Alexander George et al, *The Limits of Coercive Diplomacy*, 18-19.

[47] Alexander L. George, *Forceful Persuasion*, 5.

[48] Daniel Byman and Matthew Waxman, *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might* (New York: Cambridge University Press, 2002).

[49] Jack S. Levy, "Deterrence and Coercive Diplomacy."

[50] Alexander L. George, *Forceful Persuasion*, 20, 21.

[51] Sam Brannen, "The Return of Coercive Diplomacy," *Defense One*, September 12, 2013: http://www.defenseone.com/ideas/2013/09/return-coercive-diplomacy/70284/

[52] For an up-to-date discussion, see Stephen M. Walt, "What Would Alex George Say About Coercing Iran?" *Foreign Policy*, March 14, 2013: http://www.foreignpolicy.com/posts/2013/03/14/coercing_iran_what_would_alex_george_say.

As indicated here, force needs to be limited, focused, discrete, and credible, hinting at the consequences of continued adversarial actions. Likewise, force must be synchronized with the diplomatic actions it supports, and signal an intent not to "bludgeon," but to demonstrate "resolution," "credibility," and "determination." When Special Warfare and surgical Strike are embedded in the planning and execution of a larger political-diplomatic coercive strategy, SOF kinetic and non-kinetic effects furnish our national leadership with the necessary "psychological instrument of policy" in a strategy whose success "rests in the last analysis on psychological variables."[53]

b. Economic Aid or Coercion

Economic measures are frequently used as the means through which diplomatic engagement seeks effect. In this regard, economic aid can signal diplomatic support, and can ease the burdens on a partner country as it seeks to counter a hybrid threat. This tool has recently been used with Ukraine, by both the U.S. and EU.[54] Likewise, a whole-of-government and international approach to economic aid and capacity building has the potential to remedy short-term crises, improve government capabilities and legitimacy, and signal and enduring commitment on the part of the U.S. and its allies to the state and society under hybrid threats.[55] It may also lessen the attractiveness inside a targeted country of hybrid warfare's UW, terrorism, and organized crime activities. Of course, economic aid and capacity building—by which a country gets "skin in the game," can be among the first steps towards future military aid, in which C-UW will play a role. Finally, economic aid and capacity building in a country targeted by hybrid warfare can reduce the resource and commodity reliance of the targeted state on the adversary. This is an important consideration when states are targeted by much larger, wealthier adversaries with whom they shared a preexisting aid/trade relationship—that is, most of Russia's neighbors.

This latter contribution of economic aid to Political Warfare hints at its potential role in coercive diplomacy. Indeed, sanctions are a well-known tool of international diplomacy, targeting the economic and material capacity of pariah states to perpetuate behavior counter to international stability. Sanctions have recently been used against global powers undertaking hybrid warfare aggression—Russia in Ukraine.[56] Additionally, "coercive" aid can be used in a positive sense—to elicit or sustain activities the U.S. wishes to see from other states—or to threaten the cessation of economic assistance to states that receive it from the U.S., either through attaching political-economic conditions to the disbursement of further aid, or from interruptions, slow-downs, or reductions in aid in order to coerce changes in actions of states tending towards adversary

[53] Alexander L. George, *Forceful Persuasion*, 81.

[54] J. Weisman and D. Joachim, "Congress Approves Aid of $1 Billion for Ukraine," *New York Times*, March 27, 2014: http://www.nytimes.com/2014/03/28/world/europe/senate-approves-1-billion-in-aid-for-ukraine.html?_r=0

[55] This has been part of the "Friends of Yemen" approach. See 'Friends of Yemen' Focus on Consolidating Conditions for a Peaceful Transition," The World Bank, September 24, 2014: http://www.worldbank.org/en/news/press-release/2014/09/24/friends-of-yemen-focus-consolidating-conditions-peaceful-transition.

[56] See Sarah Graham-Brown, *Sanctioning Saddam: The Politics of Intervention in Iraq* (London: IB Tauris, 1999); "Russia Reveals Heavy Price Of Western Sanctions," *Sky News*, 24 Nov 2014: http://news.sky.com/story/1379351/russia-reveals-heavy-price-of-western-sanctions.

behavior.[57] Economic coercion and coercive aid, however, can easily be turned to the adversary state's advantage, permitting it to oppress domestic populations while diverting all resources to regime survival, while encouraging large scale transnational illicit economic activities. It is thus essential to synchronize economic aid to partnered states with coercion of others, providing "conditional inducements of a positive nature" which are viable in the local context. Given historical lessons from pre-WWII Japan, post-1991 Iraq and elsewhere, it may be that economic aid and capacity building exceeds economic coercion in Political Warfare utility, especially given characteristics of the FOE. In this regard, the 2010 *Quadrennial Diplomacy and Development Review's* recommendations regarding aid and development should be fully implemented.[58]

c. Security Sector Assistance

A security sector is composed of those institutions in a society that possess the authority to use or threaten force to protect populations, resources, territory, and common interests. It includes both military and civilian security organizations, and even those justice management and civil society organizations that have an oversight, monitoring, or policy advocacy role with respect to military and law enforcement. Most broadly, the security sector comprises "structures, institutions and personnel responsible for the management, provision and oversight of security in a country."[59] The security sector is thus much more than the military and even police, but includes multiple nodes for positive U.S. influence in support of Political Warfare objectives.

In Security Sector Assistance (SSA), the U.S. seeks to help foreign partners shape policies in the security sector and build and support military and law enforcement organizations with the capability, capacity, and effectiveness to secure national populations and resources. This assistance serves larger goals of 1) encouraging other states to address security challenges shared with the U.S.; 2) gaining greater foreign country support for U.S. regional and global interests, to include military access to airspace and basing rights, improved interoperability and training opportunities, and cooperation across a range of military, security, and diplomatic activities; 3) ensuring the spread of sociopolitical values and practices that strengthen a sovereign government and immunize it against hybrid warfare practices; and 4) strengthening collective security alliances and multinational defense organizations as a common front to oppose state and nonstate hybrid warfare.[60] Among SSA's activities are Security Sector Reform, Building Partner Capacity, and Foreign Internal Defense. All of these are mutually reinforcing, overlapping activities with an ultimately political purpose requiring tight coordination among

[57] See John Allen Gay, "Morsi and American Egypt Strategy," *The National Interest*, Feb 28, 2013: http://nationalinterest.org/blog/the-buzz/morsi-american-egypt-strategy-8168; Apratim Mukarji, *Sri Lanka: A Dangerous Interlude* (Elgin, IL: New Dawn, 2005), 26; Jason A. Kirk, *India and the World Bank: The Politics of Aid and Influence* (London: Anthem, 2011), 18; Deen K. Chatterjee, ed., *The Ethics of Assistance: Morality and the Distant Needy* (London: Cambridge University Press, 2004), 5; Anuradha Bose, Peter J. Burnell, *Britain's Overseas Aid Since 1979: Between Idealism and Self-interest* (Manchester, UK: Manchester University Press, 1991), 54-6.

[58] Department of State & USAID, *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review,* Executive Summary, 9-13.

[59] United Nations, Security Sector Reform Definitions Page: http://unssr.unlb.org/SSR/Definitions.aspx

[60] White House, Office of the Press Secretary, "Fact Sheet: U.S. Security Sector Assistance Policy," April 5, 2013: http://www.whitehouse.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy.

JIIM participants—and they all permit the U.S. and its partners to counter Hybrid Warfare and seize the initiative in Political Warfare.

(1) Security Sector Reform (SSR)

SSR is understood by the U.S. interagency as a "set of policies, plans, programs, and activities that a government undertakes to improve the way it provides safety, security, and justice" in a fashion that is "transparent, accountable to civilian authority, and responsive to the needs of the public." SSR focuses on "defense and armed forces reform; civilian management and oversight; justice; police; corrections; intelligence reform; national security planning and strategy support; border management; disarmament, demobilization and reintegration (DDR); and/or reduction of armed violence."[61] According to some, it also includes establishing or strengthening the capabilities of NGOs that support, monitor, or advocate for policy changes in the security sector. In this respect SSR considers the whole-of-government and whole-of-society as its target audience.[62]

Originally conceived in the post-Soviet context of Central and Eastern European states' transition from authoritarian to representative rule, SSR concepts were first articulated by international organizations such as the European Union, Organization for Security and Cooperation in Europe, and the UN. Additionally, national governments in Britain, Germany, and Scandinavia embraced SSR concepts, implementing programs in former Soviet regions. One aspect of SSR aligns with traditional U.S. Security Cooperation and Security Assistance, in that it focuses on improving the policy, technical, and operational competencies of all components of the security sector, at all echelons. The second, related aspect of SSR focuses on the legal, ethical, and political framework of a country's security sector, seeking to build institutions and reform practices that ensure transparency, rule of law, and respect for the human and civil rights of citizens and neighboring countries. SSR has also sought to ensure adequate civilian participation in and oversight of security sector activities. In the past decade, SSR programs have also been implemented in Latin America and Africa, with limited engagement in the Middle East.

Overall, SSR seeks to make a country's national security establishment more capable, agile, and legal, in addition to more responsive and responsible to the democratically articulated political will of its citizens. In short, SSR can gain for a country's government and security organs greater effectiveness, popular legitimacy, and suitability for international partnering. Effective SSR needs to address the whole-of-government—and thus needs to be strategized and conducted as a whole-of-government initiative by countries contributing to the effort. It must mesh the expertise and perspectives of

[61] USAID, DoD, DoS, "Security Sector Reform," Feb 2009: http://www.state.gov/documents/organization/115810.pdf.

[62] Clem McCartney, Martina Fischer and Oliver Wills, "Introduction: Dilemmas of Security Sector Reform in the Context of Conflict Transformation," Berghof Research Center for Constructive Conflict Management, Aug 2004: http://www.berghof-foundation.org/fileadmin/redaktion/Publications/Handbook/Dialogue_Chapters/dialogue2_ssr_intro.pdf; Conflict Research Unit of the Netherlands Institute of International Relations 'Clingendael', "Towards a Whole-of-Government Approach to Security Sector Reform" (The Hague, March 2008): http://www.clingendael.nl/sites/default/files/20080300_cru_occ_wog.pdf; OECD, "Security System Reform: What Have We Learned? Results and Trends from the Publication and Dissemination of the OECD DAC Handbook on Security System Reform" (2010): http://www.oecd.org/development/incaf/44391867.pdf; OECD DAC, "Conflict Prevention and Peacebuilding: What Counts as ODA?": http://www.oecd.org/dataoecd/32/32/34535173.pdf.

civilians and military personnel, and must also cultivate a civil society able to monitor and contribute to a country's security climate. If meeting its goals, SSR can immunize a country against internal dissent by addressing grievances, thus reducing the impact of subversion, insurgency, and other hybrid warfare practices. Rather than "security consumers,"[63] countries embracing SSR can act as regional Political Warfare partners, aiding neighbors' stability while serving goals shared with the U.S.

Given its political, legal, institutional, and diplomatic content, SSR is clearly an area where DOD supports other lead agencies. In the DOD realm, SSR capitalizes CF and SOF capabilities; given the latter's unique skills and inherently JIIM sensibility, SSR might even be the focus of a SOF campaign, or of the SOF contribution to the regional manifestation of a Political Warfare campaign, with significant positive impacts on a country's socio-politics and ability to support U.S. Political Warfare itself.[64]

(2) Building Partner Capacity (BPC)

Building Partner Capacity (BPC) is a Political Warfare-appropriate policy tool whose activities align with those of "security cooperation," "security assistance," and "security forces assistance."—BPC aims to "build relationships that promote specified U.S. interests, build allied and friendly nation capabilities for self-defense and coalition operations, [and] provide U.S. forces with peacetime and contingency access."[65] Including the provision of "defense articles and services in support of [U.S.] national policies and objectives,"[66] BPC concentrates on improving the "*collective* capabilities and performance" of the U.S. and current as well as emerging partners.[67] By increasing skills, agility, and capacity throughout a partner state's military, security, and police institutions, broad spectrum whole-of-government BPC enables our regional allies "to make valuable contributions to coalition operations and to improve their own indigenous capabilities."[68] As it has evolved over the past decade-and-a-half, BPC can address current allies and partners with "mature forces," or indigenous forces with "tactical shortcomings," but it can also create military and security institutions "from whole cloth" for the purposes of attaining BPC goals.[69] U.S. SOF and CF elements have registered notable successes in all three areas.

---

[63] For "security consumer" and "security provider," see Kerry Longhurst, "From Security Consumer to Security Provider: Poland and Transatlantic Security in the Twenty-First Century," *Defence Studies*, 2:2 (2002), 50-62.

[64] See Richard H. Shultz, Jr., *Security Force Assistance and Security Sector Reform* (JSOU Report 13-5, September 2013): http://jsou.socom.mil/JSOU%20Publications/JSOU%2013-5_Shultz_SFA,SSR_Final.pdf.

[65] Defense Security Cooperation Agency, "Frequently Asked Questions (FAQs)," web page, last updated August 15, 2012; also see Jennifer D. P. Moroney, D. Thaler , Joe Hogler, *Review of Security Cooperation Mechanisms Combatant Commands Utilize to Build Partner Capacity* (RAND, 2013). http://www.rand.org/pubs/research_reports/RR413.html; Jennifer D. P. Moroney, Joe Hogler, et al, *Building Partner Capacity to Combat Weapons of Mass Destruction* (RAND, 2009): http://www.rand.org/pubs/monographs/MG783.html.

[66] "Handbook for Security Cooperation Organization," http://dsca.mil/sites/default/files/1-introduction_0.pdf.

[67] U.S. Department of Defense, *Building Partnership Capacity: QDR Execution Roadmap*, Washington, D.C., May 2006, para. 1.3.1, italics added.

[68] C. Paul, C. Clarke, et al, *What Works Best When Building Partner Capacity and Under What Circumstances* (RAND, 2013), 8.

[69] LTG James M. Dubik (ret), "A Closer Look at the 'Build Partner Capacity' Mission," *Army Magazine*, January 2012: http://www.ausa.org/publications/armymagazine/archive/2012/01/Documents/FC_Dubik_0112.pdf.

In any combatant command (COCOM), BPC initiatives are expressed through a theater security cooperation plan (TSCP). The TSCP must align with local U.S. Embassy Mission Strategy and Resource Plans (MSRPs), and should consider the DoS-USAID Joint Strategic Plan (JSP) as well as the DoS's Joint Regional Strategies (JRS). This is particularly true as DoS develops the overall multi-year plan for regional security assistance, and administers related efforts in coordination with DoD.

BPC benefits from recursive relationship with SSR. As such, BPC is effective only when thoroughly coordinated among joint, interagency, and international participants. SOF thus perform a critical role in furthering BPC goals. Not only should every SOF-local partner interaction seek to build mutual capability, capacity, and interoperability, but the unique position of the theater special operations command (TSOC)—at its best, a node connecting COCOM joint force assets, the U.S. interagency, global coalition members, and local partners—enables it to function as a synchronizer of BPC activities, blending them into an overall campaign in support of a Political Warfare strategy.

(3) Foreign Internal Defense (FID)

Foreign Internal Defense consists of "participation by civilian and military agencies of a government in any of the action programs taken by another government or other designated organization to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats."[70] FID operations can combine SOF and conventional force (CF) efforts to strengthen partner states' abilities to counter an adversary state's or non-state's UW campaigns or other hybrid warfare activities within their borders, to include organized crime or cyber-attacks. Though suitable for integration with major combat operations, Iraq and Afghanistan being examples, FID efforts frequently require only a small footprint and a relatively small budget. For example, aided by 55 U.S. advisors and the expenditure of no more than $6 billion from 1980 to 1992, the El Salvadorian Government soundly defeated a communist insurgency.[71] Joint and Interagency by nature with the policies set by the Department of State as lead executive agency, FID efforts may also grow to involve all instruments of national power to support host country internal defense and development programs.[72] Likewise, U.S. FID efforts in a particular country frequently accompany those of other governments, highlighted the need for increased cross-governmental coordination and strategic synchronization.

d. Unconventional Warfare (UW)

While SSA may improve the offensive capabilities of a partner state, that is rarely the primary intent of such assistance. By contrast, UW seeks to aid directly, though with varying degrees of deniability, elements in a geographical space to oppose a governing regime or occupying power. Forms of opposition appropriate for U.S. UW support need

[70] Joint Publication 3-22: *Foreign Internal Defense*, 12 July 2010, ix.

[71] USASOC, *Casebook on Insurgency and Revolutionary Warfare Volume II: 1962 – 2009*, 27 April 2012, 117.

[72] FID tools include: indirect support including security cooperation, security assistance, multinational/joint exercises, and exchange exercises; direct support including civil-military operations, military information support operations, military training support, logistic support, intelligence, and communications sharing; and combat operations with presidential approval. FM 3-05.2: *Foreign Internal Defense*, 1 September 2011, 1-4; See also JP 3-22: *Foreign Internal Defense*, 12 July 2010, I-8, I-11.

not be violent. Rather, opposition itself moves non-linearly along a spectrum including elements of nonviolent resistance, armed resistance, insurgency, and revolution.

Nonviolent resistance can undermine a governing power's legitimacy, credibility and efficacy through protests, demonstration, sit-ins, boycotts, occupation of strategic real estate, and even the establishment of parallel institutions providing services, order, and media. While the governing power may seek to violently repress such resistance, "strategic nonviolent resistance" often further energizes state repression, while discrediting the regime internally and externally.[73] From the Indian independence movement under Gandhi to the 1991 dissolution of the Soviet Union and beyond, peaceful resistance has demonstrated its potential and its limitations. Armed resistance is not necessarily more effective than nonviolent resistance, but is characterized by the principled embrace of violence—or may emerge through disaffection with nonviolent means.

Insurgency may be an outgrowth of nonviolent resistance, or it may include the latter with multiple forms of violent activity. They key differentiator, however is the character of insurgency as "the organized use of subversion and violence to seize, nullify, or challenge political control of a region."[74] Insurgencies may emerge or proceed in various ways, but they generally seek to retain the borders of a region or state as they are, while altering its political regime—in either a transformative or restorative fashion. Insurgencies are thus not traditionally armed separatist movements in terms of goals, notwithstanding some shared tactics and effects. Likewise, while both nonviolent and armed resistance movements as well as insurgencies may in some cases seek merely to alter the policies of a governing power through pressure and coercion, armed separatism seeks to depart from that governing power's territorial authority. Of course, while differing, both insurgencies and armed separatist movements seeking secession are frequently aided by or reliant on external powers.

A revolution may be the climax of resistance and insurgency, or it may circumvent them through rapid action. Historically, revolutions have emerged as top-down coups d'état that may preserve several elements of the *ancien regime*, or through civil wars or wars against distant political overlords. Likewise, revolutions may seek merely to alter the political order of a state, or may seek far-reaching socio-political and economic changes—in this case the tail of the revolution can be quite long before the advent of a Thermidor. Frequently, revolutions alter the foreign policy and alliance orientations of the state in question, and also entail foreign involvement both in support of the revolutionary movement/regime and to aid the counterrevolution.[75]

---

[73] For nonviolent resistance, and resistance in general, see Maria J. Stephan and Erica Chenoweth, "Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict," *International Security*, 33:1 (2008), 7-44; also see idem., *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict* (New York: Columbia University Press, 2012).

[74] JP 3-24, *Counterinsurgency* 22 November 2013, I-1, II-1. In addition to Galula and Trinquier, also see Max Boot, *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present* (Liveright, 2013); Jeffrey Record, Beating Goliath: Why Insurgencies Win (Potomac Books, 2007); Richard H. Shultz, Andrea J. Dew, *Insurgents, Terrorists, and Militias: The Warriors of Contemporary Combat* (New York: Columbia University Press, 2006).

[75] For revolutions, see Charles Tilly, *From Mobilization to Revolution* (New York: Addison Wesley, 1978); idem., *European Revolutions, 1492-1992* (Wiley-Blackwell, 1996); Jeff Goodwin, *No Other Way Out: States and Revolutionary Movements, 1945-1991* (London: Cambridge University Press, 2001); Theda Skocpol, *States and Social Revolutions: A Comparative Analysis of France, Russia and China* (London: Cambridge Univ Press, 1079).

Resistance, insurgency, and revolution thus share some commonalities but differ in critical areas with regard to means, participants, and goals. While frequently incited or accelerated by U.S. and partner states' hybrid warfare adversaries, all three are eminently amenable to a whole-of-government and JIIM-enabled UW campaign enabling us to counter and deter adversary aggression. Carefully calibrated by a broader Political Warfare strategy, UW support to indigenous resistance, insurgency, or revolution can promote democratization, respect for human rights, and adherence to peaceful international norms.

(1) Traditional Unconventional Warfare

The foundational capability of Army Special Forces (SF), UW entails "activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow an occupying power or government by operating through or with an underground, auxiliary, and guerrilla force in a denied area."[76] SOF can conduct UW against a state occupying the territory of another country by enabling indigenous resistance forces to disrupt and/or eject the occupying power. SOF-conducted UW can also enable an indigenous insurgency in order to coerce, disrupt, or overthrow the government of a state acting contrary to the interests of the U.S. or its partners. In either case, SOF can conduct a UW campaign autonomously or in support of major combat operations, employing a small footprint and very low signature. Such an approach garners sympathy for resistance or insurgent groups while preserving the cloak of ambiguity regarding American involvement.

(2) Counter-Unconventional Warfare (C-UW)

Recently elaborated by retired Special Forces COL David Maxwell, C-UW connotes "operations and activities conducted by the U.S. Government and supported by SOF against an adversarial state or non-state sponsor of unconventional warfare." These SOF-supported government initiatives can "decrease the sponsor's capacity to employ unconventional warfare to achieve strategic aims."[77] More broadly, the chief advantage of C-UW is its focus on attriting an adversary's ability and will to persist in Hybrid Warfare, or to support elements of a resistance or insurgency.

A SOF-led or SOF-supported C-UW campaign can thus entail UW conducted within the territory of the state (or nonstate/parastatal entity) aiding an insurgency or separatist movement in another country—threatening the adversary's "home front" or rear area. C-UW can also include whole-of-government initiatives embracing foreign internal defense (FID) as well as improvements to law enforcement, rule of law (ROL), governance, and citizen inclusion through addressing grievances—thus shoring up the stability and legitimacy of the state and increasing its immunity to adversary UW. C-UW can also include conventional force posturing, regional and global IIA, diplomatic engagement, economic aid and sanctions—or any combination of the above.

This discussion implies that C-UW campaigns are likely "protracted and psychological-centric in nature." They should thus "comprehensively employ political, economic,

[76] Joint Publication 3-05: *Special Operations*, April 2011, II-9.

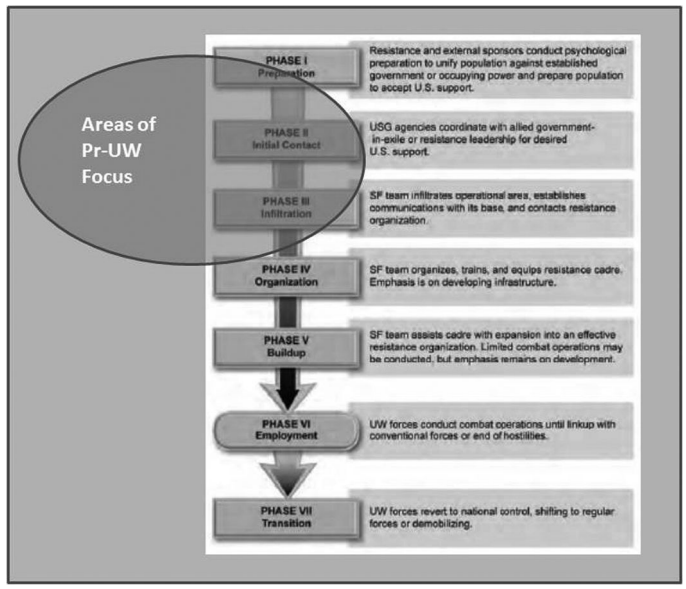
[77] David Maxwell, "Unconventional Warfare and Counter-Unconventional Warfare," (PowerPoint Presentation, United States Special Operations Command, MacDill AFB, Florida, July 9, 2014).

military, and psychological pressure" in order to degrade both the will and capability of an adversary to sponsor UW.[78] Given its "comprehensive" nature, effective C-UW requires an adaptive, holistic U.S. Government approach embracing local partners as well as operations implemented patiently through regional and global JIIM networks.

(3) UW in a Proactive Fashion (Pr-UW)

Traditional UW's definition emphasizes the endurance, if not victory, of the *local* indigenous resistance or insurgency as a metric of success; as such it may limit UW's ability to function as a strategic framework in which *U.S.* as opposed to indigenous interests are paramount. Such an indigenous-focused concern does not characterize adversary prosecution of hybrid warfare.

Additionally, American UW concepts emerged from the OSS' WWII experiences as well as from a post-war context where the Soviet Union had overrun several European states and threatened to do so to others, either through subversion or expansionist warfare. UW was thus understood as a means of response and reaction to a condition already imposed by an outside power on areas of concern to the U.S. Both in the European context as well as in later experiences in Latin America, therefore, UW was used to "fight fires."



UW in a proactive fashion is not a revision or evolution of the traditional Unconventional Warfare addressed above; rather it is an approach advocates the use of UW activities to "prevent fires" through small footprint, scaled application of force campaigns in order to develop persistent influence among potential UW constituencies; deepen understanding of significant individuals, groups and populations in the Human Domain of

[78] David Maxwell, "Unconventional Warfare and Counter-Unconventional Warfare."

the potential UW operational area; and build trust with SOF's likely UW partners in regions *before* U.S. leaders are constrained to react to crises.

UW in a proactive fashion is thus an extended duration, though low-investment, use of SOF and whole-of-government assets in a region where UW may become desirable and appropriate as conditions evolve. It can evolve establishing awareness of and non-committal relationships with political dissident groups and disenfranchised populations in states whose policies are tending towards the adversarial. In this respect, the proactive liaison with and low-visibility support to an indigenous resistance movement can be an effective counter to current or future actions counter to U.S. national interests by an adversarial governing power. If the groundwork has been laid well in advance, the ability to assist disaffected groups could influence the cost calculus of countries acting against U.S. interests. In effect, UW in a proactive fashion conducted in this fashion becomes long-term, slow-boil coercive UW, or "coercion light."

UW in a proactive fashion is thus also an enabler of a more aggressive application of UW, reducing the likelihood of a cold-start campaign in the midst of crisis. Essentially extending the first three doctrinal phases of UW, preparation, initial contact, and infiltration, far back in time while engaging in certain elements of the fourth, organizational phase, UW in a proactive fashion seeks to achieve preparation of the environment (PE) objectives with the great focus and depth implied in current doctrine.[79] Prosecuted over a period of time with whole-of-government and JIIM partners, UW in a proactive fashion allows the U.S. to gain and maintain entree to areas of concern; establish trust with significant individuals, groups, and peoples while developing allies; and ensure cognitive and moral access in the region. This kind of access requires an understanding of the physical, human, and enemy situations, and grants the legitimacy and credibility necessary to form an alliance of interests with those who could prove critical to acting against adversary elements of state and society.

Finally, and with true strategic benefit, proactive application of UW increases the likelihood of producing effects associated with coercive UW without the need to execute all phases of UW itself. By holding out the possibility of achieving traditional UW effects with a particularly small footprint, and by laying the groundwork for a more robust, better-informed conduct of UW or C-UW should the need arise, UW in a proactive fashion is therefore a fundamental component of Strategic Landpower doctrine of "rebalancing…national security strategy to focus on engagement and preventing war."[80]

e. Information and Influence Activities (IIA)

Information and Influence Activities comprise "the integration of designated information-related capabilities in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decision making."[81] The U.S. and its partners

[79] See Headquarters, Department of the Army, ATP 3-05.1: *Unconventional Warfare,* September 2013; Headquarters, Department of the Army, TC 18-01: *Special Forces Unconventional Warfare*, November 2010.

[80] USA, USMC, and USSOCOM, "Strategic Landpower: Winning the Clash of Wills," October 2013: http://www.arcic.army.mil/app_Documents/Strategic-Landpower-White-Paper-28OCT2013.pdf

[81] FM 3-13*: Inform and Influence Operations*, 25 January 2013, 1-1; HQDA, ADRP 3-0: *Unified Land Operations*, 16 May 2012.

can take advantage of many forms of IIA in its conduct of sustained whole-of-government Political Warfare. The benefit of *information*-focused activities is to build U.S. and partnered credibility among American and foreign audiences; *influence* can incline governments and populations to support JIIM Political Warfare measures and goals, reducing the ability of certain kinds of hybrid warfare activities to take root in targeted states, and decreasing the legitimacy and credibility of the government undertaking Political Warfare itself. Adhering to law, statute, and democratic norms, carefully calibrated IIA amounts to Strategic Communications: "focused USG [U.S. Government] efforts to understand and engage key audiences in order to create, strengthen or preserve conditions favorable to the advancement of USG interests, policies, and objectives . . . through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power."[82]

(1) Public Affairs (PA)

Public Affairs (PA) is a critical mission area for both the DoD and Interagency Departments. PA resides clearly on the "information" side of the information-to-influence spectrum, and the primary audience for PA activities is the American population resident in the homeland and abroad. For the DoD, PA seeks to keep the American people informed of activities, initiatives, and operations, chiefly by interfacing with U.S. media outlets, though engagement with international media is also the norm. DoD PA also addresses the members of the uniformed services. Additionally, by informing "domestic and international audiences of joint operations to support combatant command public information needs,"[83] DoD PA "helps to establish the conditions that lead to confidence" in the Joint Force "and its readiness to conduct operations in peacetime, conflict, and war."[84]

DoS PA is likewise information-focused, with a primarily American audience but a definition of "public" to include non-U.S. audiences. Through timely and accurate information, the DoS Bureau of PA's mission includes "furthering U.S. foreign policy and national security interests as well as broadening understanding of American values." The Bureau's "strategic and tactical communications planning to advance America's foreign policy interests" results in press briefings, media outreach at home and abroad, use of social media "to engage the public," coordination of regional media hubs "for engagement of foreign audiences," arranging community-level interactions for Americans to discuss U.S. foreign policy, and preparing products for the Department abroad.[85]

Both military and civilian agencies' PA are bound by law and mission to produce information as accurately as possible, as opposed to disinformation and propaganda. Likewise, primary audiences have traditionally been U.S. citizens, civilian and military. Yet, PA does serve a role in furthering our national security through its dissemination of information, and may address foreign audiences. It specifically addresses citizens, and can thus serve a function in bolstering popular confidence in governments with

[82] JP 3-13, IO, GL-12.

[83] JP 3-13, II-8.

[84] See U.S. Army Public Affairs Wepbage: http://www.army.mil/info/institution/publicAffairs/; also see U.S. DOD "Principles of Information" Webpage: http://www.defense.gov/admin/prininfo.aspx.

[85] See U.S. Dept of State, Bureau of Public Affairs Webpage: http://www.state.gov/r/pa/index.htm.

whom the U.S. seeks to partner through security sector assistance and other means to defeat adversary hybrid warfare. As PA can incline both domestic and foreign populations towards a positive view of U.S. activities through its commitment to accurate information, it can also encourage foreign populations to support U.S. efforts and those of their governments, thus reducing the appeal of hybrid warfare enticements, such as organized crime, political subversion, and insurgency. To achieve a fully integrated approach, the U.S. should reestablish the United States Information Agency (USIA).

(2) Public Diplomacy

U.S. statute, policy, and civil-military norms designate the Department of State as the lead in the USG public diplomacy mission.[86] DoS and affiliated agencies understand PD as the effort to "understand, inform, engage and influence global audiences, reaching beyond foreign governments to promote greater appreciation and understanding of US society, culture, institutions, values and policies" through means including "international exchanges, international information programs, media research and polling, and support for nongovernmental organizations."[87] In supporting interagency initiatives, DOD Joint Publication 3-13 defines PD as overt government activities "to promote United States foreign policy objectives to understand, inform, and influence foreign audiences and opinion makers, by broadening the dialogue between American citizens and institutions and their counterparts abroad."[88] More broadly, scholarly observers of American PD have described it as "the conduct of international relations by governments through public communications media and through dealings with a wide range of nongovernmental entities . . . for the purpose of influencing the politics and actions of other governments."[89]

These definitions emphasize the role of PD as communicating with and influencing foreign populations, to include officials, in order to influence the foreign policy decisions and actions of governments. By nature and law addressing foreign populations only, it is the tool through which the entire USG can connect with significant individuals, groups, and populations in foreign areas, in order to activate and sway attitudes in favor of U.S. interests, and, if necessary, against the actions of adversary governments, as regards either domestic or foreign policies. While PA is invaluable in strengthening American's moral resolve to support sustained Political Warfare by honestly and persistently informing our citizens of what the USG does, PD is indispensable in the prosecution of Political Warfare abroad, explicitly seeking to influence foreign populations and officials to support friendly governments in the pursuit of policies and actions aligned with U.S. goals. As presented here, PD is also a natural tool of coercive diplomacy.

---

[86] See Title 22, Section 2732, United States Code. Also see Department of Defense Directive No. 3600.01. Accessed from http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf.

[87] American Academy of Diplomacy, *A Foreign Affairs Budget for the Future: Fixing the Crisis in Diplomatic Readiness* (October, 2008), 24; U.S. Advisory Commission on Public Diplomacy, "Consolidation of USIA Into the State Department: An Assessment After One Year," (2000), 5.

[88] U.S. Army War College, Information Operations Primer: Fundamentals of Information Operations, 2011: http://www.au.af.mil/au/awc/awcgate/army-usawc/info_ops_primer.pdf, 12; *U.S. Department of Defense, DOD Dictionary*, http://www.dtic.mil/doctrine/jel/doddict/data/p/11548.html.

[89] Alan K. Henrikson, April 2005, cited on "Definitions of Public Diplomacy" Webpage, Fletcher School, Tufts University: http://fletcher.tufts.edu/murrow/diplomacy/definitions.

While by law the Secretary of State is responsible for all government programs engaging foreign audiences,[90] other government agencies of course support this task through the ways they influence foreign attitudes in their daily interactions with foreign governments and populations. In this respect DoD components have had a notable role in aiding overall USG PD initiatives through its own statutorily authorized IIA activities—but perhaps even more so through the narrative communicated by its security cooperation, civil-military operations, and other sustained engagement activities with civilians, law enforcement, military personnel, and government officials abroad. It is critical that DoD and other agencies ensure PD initiatives are aligned with the authorities, themes, and guidelines of DoS PD. Within that rubric, aggressive DoD support to PD aids all the Political Warfare initiatives in this paper. Given the consistent, intense interaction between globally deployed SOF personnel and host country citizens and officials, it is critical that SOF soldiers act with a PD sensibility. Army Special Operators should therefore be included in PD planning and execution as valuable connective tissue among USG agencies.

(3) Cognitive Joint Force Entry (CJFE) and Military Information Support Operations (MISO)

A recent addition to the SOF conceptual arsenal, CJFE seeks to produce strategic effects in the preparation and shaping phases of an operation by inclining foreign populations to favorably view U.S. activities. Intended to achieve persistent influence, CJFE "synchronizes and employs all components of the global information environment," in order to conduct "information and influence activities to shape the environment beginning in pre-conflict stages." Two principles integral to CJFE are Cognitive Depth and Cognitive Security. The former encompasses "a population's realm of perceptions, beliefs, opinions, and attitudes," while the latter constitutes "as a condition in an operating environment where favorable opinions and perceptions within a populace reduce risk to the force and to the mission. It is characterized by a non-hostile, neutral, or supportive disposition for current and future US activities." By accessing an environment's Cognitive Depth through "a persistent, continuous awareness of the global information environment, which provides the ability to anticipate challenges and identify opportunities for early and responsive actions," SOF is able to attain Cognitive Security.[91]

CJFE is a highly relevant enabling concept and functional component of C-UW, UW in a proactive fashion, and the overarching concept of Political Warfare. By conducting IIA aligned with CJFE ideas, SOF can support the whole-of-government effort to decrease the cognitive and affective commitment to UW among key adversary constituencies. These include government and military officials of the adversary state conducting UW; individuals, groups and populations considered critical by the adversary regime; and the adversary state's proxies seeking to undermine a state supported by the U.S.

Tools to effect this include military information support operations (MISO). These encompass "integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or

[90] "Department of State maintains the lead for public diplomacy with the DOD in a supporting role." Department of Defense Directive No. 3600.01. Accessed from http://www.dtic.mil/whs/directives/corres/pdf/360001p.pdf.

[91] See USASOC, "Cognitive Joint Force Entry White Paper," 26 Sept 2014, 4-5, 7.

usurp the decision-making of adversaries and potential adversaries."[92] MISO pursues these goals in part by communicating "selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals,"[93] ultimately "to support U.S. national objectives."[94] With due regard to law and authorities, MISO is quite able to support PD activities in friendly and adversary regions.[95]

At the same time, CJFE can bolster the willpower of partner governments and populations with whom the U.S. is partnering to counter adversary messaging. In the context of UW in a proactive fashion, CJFE-informed IIA will contribute to preserving moral access among potential UW partners will also diminishing the will to persist in adversarial actions on the part of the government targeted by UW in a proactive fashion. Finally, CJFE is critical to Political Warfare given the ideological content and leverage inherent in effective IIA, as well as the concept's emphasis on efforts prior to war, in order to "win population-centric conflicts, oftentimes, and preferably, before they start."[96]

f. The Human Domain (HD)

Initiated by US Special Operations Command (USSOCOM), the HD concept understands the operating environment as a synergistically interactive combination of several "domains": land, air, sea, cyber, and human. The Human Domain focuses on people, in terms of "their perceptions, decision-making, and behavior." HD understands people as "individuals, groups, and populations" (IGP) who exercise agency within the area of operations or beyond it in a way that can impact U.S., partner, and adversary interests. "The success of any strategy, operation, or tactical action depends on effective operations in the human domain," and that effectiveness, in turn, hinges on identifying and influencing relevant IGPs to support U.S. goals.[97] While it's the case that in some campaigns the Human Domain is of secondary or little concern, it is also the case that in population centric conflicts, it is a primary concern.

HD's five principal "elements" and related "considerations" shape human decision-making and behavior and provide insight into the "culturally relevant and credible sources of legitimacy" on which the Joint Force seeks to draw. By evaluating and fully comprehending these HD elements, SOF and the broader Joint Force will prove "capable of shaping human decision-making and associated behavior to create desired effects."[98] As such, understanding the manifestation of HD elements and considerations in an area of potential operations is crucial to effective Political Warfare activities, just as such an

[92] JP 3-13, GL-3

[93] JP 3-13, II-9; also see DOD Directive S-3321.1, "Overt Psychological Operations Conducted by the Military Services in Peacetime and in Contingencies Short of Declared War", as discussed in Daniel Silverberg, and Joseph Heinmen, "An Ever-Expanding War: Legal Aspects of Online Strategic Communications." *Parameters* (Summer 2009).

[94] See FM 3-05.30: *Psychological Operations*, April 2005 ://fas.org/irp/doddir/army/fm3-05-30.pdf

[95] http://www.soc.mil/swcs/swmag/archive/SW2401/SW2401TheFutureOfMISO.html

[96] COMUSSOCOM's *Posture Statement to the House Armed Services Committee*, 11 Mar 2014.

[97] USSOCOM, *Operating in the Human Domain* Version 0.70 (5 September 2014), iii, 10, 22, 52; ii, iii, 1, 2, 6, et passim.

[98] USSOCOM, *Operating in the Human Domain*, 7, 8, 2.

understanding is furthered by long-duration UW. More broadly, the emphasis placed on "psychological variables" by theoreticians of coercive diplomacy, "the importance of actor-specific behavioral models of adversaries," points to a "situational analysis" by all whole-of-government participants in Political Warfare, which HD enables and requires.[99]

Human Domain Elements			
HD Element	**Description**		
Social	The structure and relationships among groups and institutions, involving competition for influence and efforts to impose interest and perspectives.		
Cultural	Impact of a society's beliefs, customs, way of life on people's behavior.		
Physical	How the natural and manmade world shapes individuals' priorities.		
Informational	The sources, availability, and substance of data.		
HD Element	**Consideration / Sub-Area**		
Social	➢ Public Groups ➢ States Institutions [sic] ➢ Local Government		➢ Civic Groups ➢ Societal Groups
Cultural	➢ Ideology ➢ Tribalism ➢ Customs and Beliefs ➢ Ethnicity		➢ Religion and rituals ➢ Language ➢ Communication
Physical	➢ Geography ➢ Topography ➢ Hydrology		➢ Urbanization ➢ Resources ➢ Climatology
Informational	➢ Means	Internet Print Radio Television Person-to-Person	➢ Message ➢ Audience
Psychological	➢ Cognition	Awareness Perception Reasoning	➢ Judgment ➢ Emotion ➢ Critical Thinking

g. Political Warfare

In its simplest form, contemporary Political Warfare combines traditional and novel forms of Special Warfare described in this paper, along with SSA and IIA informed by an overall diplomatic approach integrating persuasion, coercion, and aligned economic measures. All these pillars, military and otherwise, are founded on a mastery of the Human Domain and enabled by Cognitive Joint Force Entry. Though UW's forms, SSA, and IIA may be conducted autonomously or led by SOF, Political Warfare attains full effect when featuring the full breadth of JIIM contributors *supported* by SOF, with SOF elements acting, perhaps as the JIIM integrator.

[99] Alexander George, "The need for Influence Theory and Actor-Specific Behavioral Models of Adversaries," in B. R. Schneider & J. M. Post, eds., *Know thy Enemy: Profiles of Adversary Leaders and their Strategic Cultures* (Maxwell Air Force Base, AL: U.S. Air Force Counterproliferation Center, 2002).

Twenty-first-century Political Warfare bears much in common conceptually with Kennan's mid-twentieth-century articulation of "the employment of all the means at a nation's command, short of war, to achieve its national objectives," though with some updating. Indeed, the Political Warfare of the emerging and future operating environments features "shadow conflicts, fought by masked warriors often without apparent state attribution,"[100] in addition to "wars of silicon," where states and nonstate actors will employ "cutting-edge technology, advanced military capabilities, and substantial financial resources" to "unbalance and unhinge" states "by undercutting civil and military capabilities"[101] as a means to intimidate the U.S. or its regional partners during "peacetime."

Still, an enduring conceptual aspect of Political Warfare is the use of DIME-FIL tools without the direct engagement of military forces for destructive purposes. Embracing persuasion and coercion, as part of "the art of heartening friends and disheartening enemies, of gaining help for one's cause and causing the abandonment of the enemies',"[102] Political Warfare prioritizes "the use of words, images, and ideas."[103] In the later stages of the Cold War, the U.S. went beyond use of various "colors" of propaganda,[104] and facilitated the establishment of non-governmental organizations whose goals in supporting democratization of politics and media in foreign regions aligned with overall anti-Soviet U.S. policy.[105]

Of course, throughout its history, Political Warfare has allowed for using means at higher levels of risk, to include covert operations and influence, to influence outcomes, discourage certain behaviors, or change the regime itself, hence the close relationship between forms of UW and Political Warfare itself.[106]

In this regard, the WWII-era British Government Political Warfare Executive's "precepts of political warfare" constitutes a trenchant, enduring definition of Political Warfare as "the systematic process of influencing the will and so directing the *actions* of peoples in" adversary and adversary-targeted regions, "according to the needs of higher strategy." Political Warfare's "primary aim is to assist the destruction of the foundations" of the adversary state's capacity to obstruct U.S. and partnered interests, in order to "break

[100] LTG David Barno (ret), "The Shadow Wars of the 21st Century," *War on the Rocks*, July 23, 2014: http://warontherocks.com/2014/07/the-shadow-wars-of-the-21st-century/.

[101] LTG David W. Barno (ret), "Silicon, Iron, and Shadow: Three Wars that will Define American's Future," *Foreign Policy*, March 19, 2013: http://www.foreignpolicy.com/articles/2013/03/19/silicon_iron_and_shadow

[102] Angelo M. Codevilla, "Political Warfare: A Set of Means for Achieving Political Ends," in Waller, ed., *Strategic Influence: Public Diplomacy, Counterpropaganda and Political Warfare* (IWP Press, 2008), 218: http://jmw.typepad.com/pdpw/files/codevilla_chapter.pdf

[103] Paul A. Smith, *On Political War* (Washington: National Defense University Press, 1989), 7.

[104] "White" propaganda emerges overtly, from a known source. "Gray" propaganda is the "semiofficial amplification of a government's voice." See Angelo Codevilla and Paul Seabury, *War: Ends and Means* (Washington, DC: Potomac Books, Inc., 2006), 157. "Black" propaganda "appears to come from a disinterested source when in fact it does not," originating instead from an unknown, deniable source sympathetic to the government whose claims it advances. See Angelo M. Codevilla, "Political Warfare: A Set of Means for Achieving Political Ends," 219.

[105] Robert Ree, "Political Warfare Old and New: The State and Private Groups in the Formation of the National Endowment for Democracy," *49th Parallel*, 22 (Autumn 2008), 22.

[106] Paul W. Blackstock, *The Strategy of Subversion: Manipulating the Politics of other Nations* (Chicago: Quadrangle, 1964).

the will to" sustain actions contrary to U.S. desires. Political Warfare's "ultimate aim is to win the 'War of Ideas,' which is not conterminous with hostilities." Political Warfare requires "co-operation of the [armed] services, aggressive diplomacy, economic warfare and the subversive field-agencies, in the promotion of such policies, measures or actions needed to break or build morale." Finally, Political Warfare "must be geared to strategy."[107]

[107] His Britannic Majesty's Government, Political Warfare Executive, "The Meaning, Techniques and Methods of Political Warfare," London, 1942: http://www.psywar.org/psywar/reproductions/MeanTechMethod.pdf. The full Political Warfare Appendix:

Appendix A
I. Precepts of Political Warfare

Definition.

(1) Political Warfare is the systematic process of influencing the will and so directing the *actions* of peoples in enemy and enemy-occupied territories, according to the needs of higher strategy.

Function.

(2) Political Warfare is the Fourth Fighting Arm an instrument of which is PROPAGANDA and its forces are the dissident elements, potentially or actually existing within the ranks of the enemy and the sympathizers potentially or actually militant in enemy-occupied countries.

(3) Political Warfare's primary aim is to assist the destruction of the foundations of the enemy's war machine in conjunction with military action, in order to break the will to war of the enemy nation. It promotes disaffection, resistance and active co-operation amongst the enemy's military, civil and industrial population, and amongst the subject peoples.

Aims.

(4) Political Warfare's further aim is to ensure that, in conjunction with Allied military intervention, organised elements of resistance and disruption will hasten the collapse of the enemy's forces.

(5) Political Warfare's ultimate aim is to win the "War of Ideas" which is not conterminous with hostilities.

6) Political Warfare requires for the fulfilment of those aims the co-operation of the three Fighting Services, aggressive diplomacy, economic warfare and the subversive field-agencies, in the promotion of such policies, measures or actions needed to break or build morale.

Requirements.

(7) Political Warfare requires for the fulfilment of those aims, the mutual confidence of the Foreign Office, the Fighting Services, the Ministry of Economic Warfare and other agencies and, with due regard for security, the disclosure of such secret plans, intelligence or policies as are necessary for its operations.

General Operations.

(8) Political Warfare operates overtly (i.e., through "open" broadcasting) and covertly (through "black" agencies) but its strategy and tactics must be as secret as those of the other Fighting Services, requiring therefore the same protection and security.

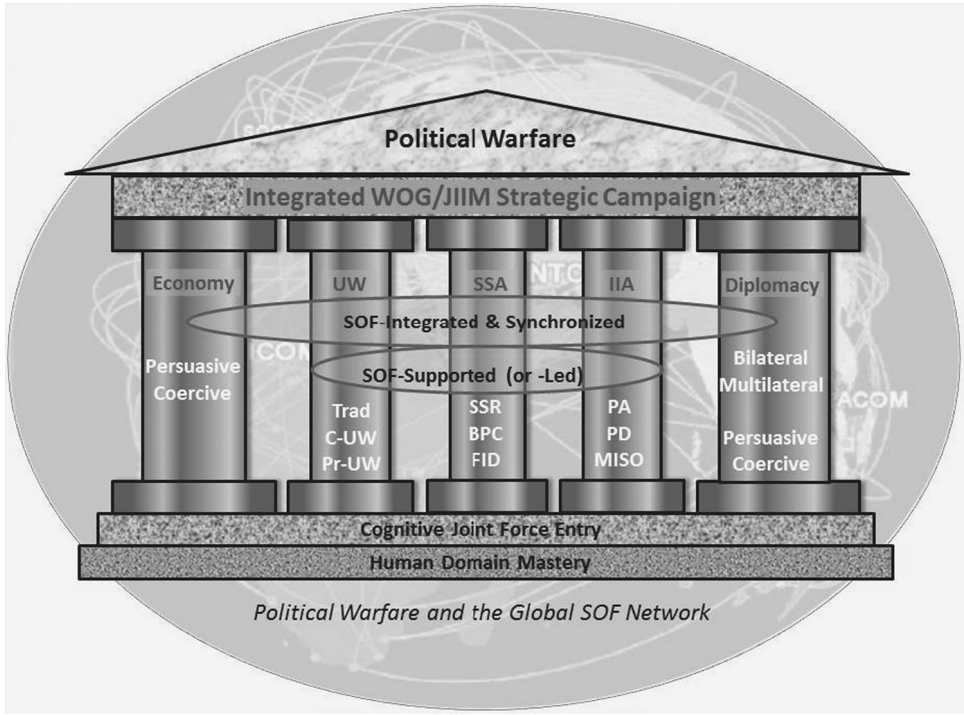
Specific Operations.

(9) Political Warfare has a further service to render to the higher strategy, through its experts who, by thorough knowledge of the population and conditions in the regions in which they specialise, can assist in the preparation for specific military operations.

(10) Political Warfare must be geared to strategy, continually linked to, and in consultation on, the day to day conduct of the war.

United Operations.

11) Political Warfare in the totality of war must combine with all similar activities of the United Nations.



Advancing the concept of Political Warfare will require that practitioners clearly understand U.S. authorities and international law. In terms of U.S. authorities, there is widespread confusion regarding Title 10 and Title 50 authorities, traditionally associated with DOD and intelligence agencies, respectively. Specifically, "the Title 10 -Title 50 debate is the epitome of an ill-defined policy debate with imprecise terms and mystifying pronouncements"[108] The current debate suggests that pursuing political warfare will include addressing U.S. authorities such as Title 10 and Title 50. Similarly, potential challenges related to the interpretation of international law may impact political warfare. For example, "the international law principle of non-intervention prohibits states from using coercive means to intervene in the internal or external affairs of other states."[109] In that context, "the United States has consistently interpreted the U.N. Charter to ban nearly all foreign support to insurgencies, believing that any assistance beyond non-discriminate humanitarian aid would constitute a use of force in violation of Article 2(4)" of the Charter.[110] But conditions have changed, and "this fundamentalist approach, while understandable in the context of the Cold War and the spread of communism, arguably lacks salience in the twenty-first century and runs counter to much

[108] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, and Covert Action," *Harvard National Security Journal* 85, no. 3 (2011), 86.

[109] Michael N. Schmitt and Andru E. Wall, "The International Law of Unconventional Statecraft," *Harvard National Security Journal*, no. 5 (2014), 353.

[110] Michael N. Schmitt and Andru E. Wall, "The International Law of Unconventional Statecraft," *Harvard National Security Journal*, no. 5 (2014), 371.

state practice."[111] What is also clear is the recognition that the activities aligned with Title 10 and Title 50 are becoming 'increasingly similar,' which has contributed to the challenge.[112] For example, due to their potentially perceived nature and character, activities associated with Unconventional Warfare could require nuanced interpretation to parse the lines of authority. In both U.S. policy and international law, the community of practitioners will need clarity to advance the cause of political warfare.

3-4. Centrality of SOF to Political Warfare

Among the Joint Force's Components, SOF, and SOF now with an operational level vote, are ideally suited to advocate for, integrate, and synchronize the military components of Political Warfare efforts, due to unique operational capabilities, a historically thoroughgoing embrace of WOG approaches, and persistent regional and global engagement, with local state, substate, and international coalition partners.

a. Catalyzing Whole-of-Government Synergies

Inspired by the *ARSOF Operating Concept* and the USSOCOM *SOF Operating Concept*, an embrace of the interagency through meaningful, synergistic partnerships is part of SOF's DNA. SOF personnel actively seek to bridge "critical seams among SOF, CF, and interagency partners," in order to catalyze and sustain whole-of-government initiatives providing U.S. policymakers a continuum of options based on a "blending of capabilities between the DOD and the interagency."[113] In the same vein, the temperament, education, and training of SOF personnel drive them to seek and combine the expertise "resident across SOF, U.S. Government agencies, nongovernment organizations, academia, and think tanks,"[114] through enduring personal relationships, operational collaboration, or Special Operations Support Teams assigned by SOCOM "to every appropriate U.S. Government department and agency to coordinate, collaborate, and synchronize SOF operations and activities with those of the host department or agency."[115] Likewise, in recent deployments, "SOF developed plans in coordination with the host governments and integrated them into the mission strategic plan of the Chief of Mission ("Country Team") and the theater campaign plan of the Geographic Combatant Commander," with SOF representatives currently available to "every appropriate" U.S. diplomatic mission abroad.[116] Therefore, just as SOF's Political Warfare core competencies are inherently whole-of-government in nature, SOF seeks to strengthen the whole-of-government network by acting as its connective tissue.

[111] Michael N. Schmitt and Andru E. Wall, "The International Law of Unconventional Statecraft," *Harvard National Security Journal*, no. 5 (2014), 371.

[112] Andru E. Wall, "Demystifying the Title 10-Title 50 Debate: Distinguishing Military Operations, Intelligence Activities, and Covert Action," *Harvard National Security Journal* 85, no. 3 (2011), p. 139.

[113] USASOC, *ARSOF Operating Concept 2022*, 15.

[114] USASOC, *ARSOF Operating Concept 2022*, 16.

[115] USSOCOM, *Special Operations Forces Operating Concept*; JP 3-05: *Special Operations*, III-02.

[116] USSOCOM, *Special Operations Forces Operating Concept*, 4, 9.

b. SOF's Regional and Global Engagement

SOF's commitment to Joint and Interagency partnerships functions as a stepping stone to the kind persistent relationships with regional and global partners necessary to enable and sustain effective Political Warfare activities. In order to "protect and advance U.S. national interests in an unstable, complex, and transparent world," SOF seek "enduring and sustainable" international cooperation through forces "postured forward to engage with their strategic partners and build and sustain enduring partnerships."[117] Forward-postured SOF elements engage at the local-through-national level of foreign areas, in order to "build relationships that enable SOF to work with and through partners" to meet common challenges while serving broader U.S. national security interests. Likewise, these elements function "autonomously in urban environments as well as austere and remote locations, without any degradation in their capabilities or support."[118]

Living and operating with foreign counterparts, SOF operators "avoid creating large footprints, disrupting local economic and civil conditions, and causing damage to their partners' narratives."[119] Indeed, "foreign partners will at times be more willing to work with SOF due to their small footprint in politically and/or diplomatically sensitive environments."[120] Preserving the legitimacy of local partners and the credibility of the U.S., SOF teams prepare the environment to meet the challenges of potential crises and conflicts. These kinds of SOF activities themselves constitute ongoing Political Warfare. Yet, through focus on three main kinds of international partners: foreign SOF, foreign conventional armed forces and security forces, and foreign irregular forces, groups, or individuals, SOF's enduring regional engagements also provide the proactive basis for more active Political Warfare through PR-UW, C-UW, FID, and IIA.

In order to obtain maximum operational and strategic effect in support of U.S. policy goals, SOF activate whole-of-government and broader JIIM partnerships through Theater Special Operations Commands (TSOCs) under the operational control of geographic combatant commanders (GCCs). TSOCs, in turn, function as geographical nodes in the Global SOF Network (GSN), a "globally linked force" of SOF and their JIIM, non-governmental, commercial, and academic partners. Envisioned as a "living and learning system that remains agile, responsive, and adaptable as the strategic environment evolves," the GSN exploits "an interdependent web of networks operated by strategic partners," to include those with high-end SOF, CF, and intelligence capabilities, including those from regional and local partners.[121] While it might provide the SOF component to an envisioned "global landpower network,"[122] the GSN's network of networks enables a shared consensus regarding the strategy and implementation of proactive Political Warfare able to counter and deter hybrid warfare conducted by state and

[117] USSOCOM, *Special Operations Forces Operating Concept*, 3.

[118] Ibid., 7.

[119] Ibid.

[120] Joint Publication 3-05 *Special Operations*, I-2.

[121] USSOCOM, *Special Operations Forces Operating Concept*, 3; Joint Publication 3-05 *Special Operations*, III-2.

[122] See Charles T. Cleveland, (LTG) and Stuart L. Farris (LTC), "Toward Strategic Landpower," *Army* , July 2013; Cleveland and Farris, "A Global Landpower Network Could be the Ultimate Anti-Network," *Army*, August 2014; Paul McLeary, "US Army Working with Joint Chiefs to Develop 'Global Landpower Network'," *Defense News*, Mar 13, 2014: http://www.defensenews.com/article/20140313/DEFREG02/303130034/US-Army-Working-Joint-Chiefs-Develop-Global-Landpower-Network-.

nonstate adversaries targeting the U.S., its at-risk regional partners, and critical NATO alliance members.

As such, SOF consider GSN-embedded steady-state relationships with JIIM partners, and operations maximally integrated with reliable state and nonstate foreign partners, to be a cornerstone of the SOF sensibility and an extension of the SOF role as the integrating connective tissue supporting the interagency solution.[123] Such relationships and the sensibility producing them are also critical to successful prosecution of long-term, patient, Political Warfare.

c. SOF's Unique Operational Capabilities

Over the past several decades, SOF have cultivated and sustained an exquisite level of expertise in capabilities critical to effective Political Warfare. Though known for its Surgical Strike ability to engage global targets with discriminating precision, it is in the realm of Special Warfare that SOF makes its focal Political Warfare contribution. An "umbrella term indicating operating force conduct of combinations of" UW, FID, IIA, counterterrorism and COIN "through and with indigenous personnel," SOF's Special Warfare features "discreet, precise, politically astute, and scalable capabilities" enabling "politically sensitive missions over extended periods of time in hostile, austere, and denied environments." In this respect , SOF's "deep language and cultural expertise" permits "influence over the human domain in pursuit of U.S. objectives," while a "proficien[cy] in…building indigenous forces, alongside which they will fight in permissive, uncertain, and hostile environments" renders Army special operators well adapted to the performance of Political Warfare activities described in this paper.[124]

More broadly, throughout the SOF enterprise, we have organizations and senior leaders that now have developed expertise in Political Warfare at the Campaign Level. Additionally, SOF operators "are exceptionally well-educated, expertly trained…and are critical thinkers, eager to embrace new cultures and understand different ways of thinking. They master interpersonal and social networking skills, knowledge, and understanding that allow them to operate fluidly within diverse non-Western societies." SOF personnel also understand "the impact and influence that human behavior has across all domains" as well as "the consequences that actions in other domains have on human behavior." Finally, "They train others in these skills and, in the process, convey the U.S. perspective in a favorable manner that influences partners, adversaries, and relevant populations."[125] SOF are thus ideal partners in whole-of-government Political Warfare.

4. Solution Concepts and Components

a. Develop Concepts and Doctrine

In order for DOD, particularly SOF, to successfully fulfill its mission in a US Political Warfare Strategy to be fully integrated as an SOF, Army, and larger Joint Force capability,

[123] See Chuck Ricks, ed., *The Role of the Global SOF Network in a Response Constrained Environment* (JSOU, November 2013): https://jsou.socom.mil/JSOU%20Publications/Global%20SOF%20Network%20Resource%20Constrained%20Envir onment_FINAL.pdf.

[124] USASOC, *ARSOF Operating Concept 2022*, 26 September 2014, 11.

[125] USSOCOM, *Special Operations Forces Operating Concept*, May 2013, 10.

the family of Joint Operations Concepts (JOpsCs) as well as existing relevant Joint Operating Concepts (JOCs) require review, both with regard to their current integration of UW and other Political Warfare-affiliated ideas, as well as with the intent to revise the relevant them to reflect C-UW, Pr-UW, and IIA informed by CJFE. In the process these Political Warfare components themselves need to be elaborated further to ensure harmonization with validated Joint concepts. Ultimately, it may be warranted to develop a JOC along the lines of the Joint Concept for Integrated Campaigning (JCIC).

Subsequent to this review and development of appropriate JOpsCs and JOCs, joint doctrine should be revised at the keystone and subordinate levels, with a focus on the Joint Operations (JP 3-0) and Joint Operation Planning (JP 5-0) series of publications. This revision of joint doctrine should be informed by, and assist the revision of service-and SOF-specific doctrinal and technical publications, in the latter case, with a focus on integrating Political Warfare with broader SOF concepts and principles.

b. Develop Strategies

We have seen that the future operating environment will feature state and nonstate competition for regional and global influence, frequently in the form of ideological battles in the human domain. Political Warfare should thus be scoped as an integrating strategy enabling the U.S. to influence local struggles in a positive direction, and policies should be developed assigning Political Warfare as a core mission of government agencies responsible for UW and associated Political Warfare doctrines and capabilities.[126] Several synergistic initiatives serve this goal:

1) Establish Political Warfare Strategies. Strategies need to emphasize both overt and covert activities across all government agencies "short of war,"[127] as well as the requirement for approaches nested through multiple echelons. Political Warfare strategies and policies must be planned, coordinated, and synchronized from the strategic national level down to the tactical level. To ensure horizontal synchrony and vertical nesting, an NSC director for political warfare or C-UW activities could oversee development of policies and directives; prioritize efforts and manage interagency concerns; coordinate activities and funding across the government; and provide oversight for the implementation of Presidential Policies or Directives. The Department of State would be the lead for political warfare and C-UW activities, with other Departments and Agencies in a supporting role.[128] The Department of

[126] Max Boot, Jeane J. Kirkpatrick, Michael Doran, and Roger Hertog, "Political Warfare."

[127] There are many such "short of war" activities. The following comprises a sampling:

- Economic sanctions against countries, groups, and individuals, as well as coercive trade policies
- Diplomacy, including boycotting international events, establishing treaties or alliances to counter adversary UW, severing diplomatic relations, or excluding offending states from membership in international forums
- Support for "friendly" insurgent groups to coerce, disrupt, or overthrow an adversary regime,
- Support for friendly governments to counter adversary political warfare activities,
- Support for foreign political actors and parties opposing adversarial regimes
- Strategic communications and information operations to expose adversary activities.

[128] Kennan is again suggestive in this regard. At the strategic level, he recommended a covert political warfare operations directorate or board under the NSC Secretariat, with the director designated by and

Defense should be the lead for building a Global Land Power Network (GLN) to enable the development of these strategies and their application.

2) Designate a Lead Organization to Coordinate and Synchronize Efforts at the National and Deployed Echelons. Though whole-of-government, Political Warfare efforts must have a designated lead organization to coordinate and synchronize planning and execution to achieve unified action. Presidential Policy Directive (PPD) 23 *U.S. Security Sector Assistance Policy* affirms that to strengthening allies and partner nations, officials must "foster United States Government policy coherence and interagency collaboration" through a form of "transparency and coordination" able to promote "broader strategies, synchronize agency efforts, [and] reduce redundancies."[129] The current counterterrorism apparatus may thus provide a useful example of what might serve for Political Warfare. Max Boot et al, suggests a Political Warfare apparatus would entail:

- Assigning a political warfare coordinator in the National Security Council (NSC),
- Creating a strategic hub, an interagency coordinating body that pulls all of the local efforts together, in the State Department
- Creating political warfare career tracks in the Department of State (DOS), Department of Defense (DOD), U.S. Agency for International Development (USAID), and the Central Intelligence Agency (CIA).[130]

Given State Department leadership in C-UW, in appropriate countries, the U.S. country team should be the focal point to plan, coordinate, and synchronize political warfare and C-UW activities. Led by the Ambassador, the country team will develop specific country plans and strategies for U.S unilateral activities, integrating host nation activities to obtain mutual objectives.

The National Security Council system would then ensure the coordination and synchronization of strategic political warfare and C-UW policies and directives among theater and operational level organizations, in cases where unconventional warfare is a threat. In turn, the Geographical Combatant Command would coordinate and synchronize political warfare and C-UW activities within a region. This would occur through the Joint Interagency Coordination Group (JIACG), staffed with DOD personnel and representatives of other Departments and Agencies who strive to collaborate, plan, and synchronize interagency efforts to achieve U.S. objectives.[131] At the lower tactical level of command or task force level, the interagency coordi-

responsible to the Secretary of State. In this approach, the directorate's staff would be divided equally between State Department and Defense Department representatives selected by the Secretaries, and the directorate would have complete authority over covert political warfare operations. George Kennan, "Policy Planning Memorandum," May 4, 1948, National Archives and Records Administration, RG 273, Records of the National Security Council, NSC 10/2, accessed June 9, 2014, http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm.

[129] The White House, Office of the Press Secretary, "Fact Sheet: U.S. Security Sector Assistance Policy," The White House, April 5, 2013, accessed July 3, 2014, http://www.whitehouse.gov/the-press-office/2013/04/05/fact-sheet-us-security-sector-assistance-policy.

[130] Max Boot, Jeane J. Kirkpatrick, Michael Doran, and Roger Hertog, "Political Warfare."

[131] United States Joint Forces Command, *Commander's Handbook for Joint Interagency Coordination Group*, 1 March 2007, II-1.

nation can be exercised through Liaison Officers (LNOs) dispatched from selected Departments or Agencies for specific mission purposes.[132]

3) Leverage SOF Special Warfare and Surgical Strike Capabilities. Within DOD, SOF is a key component of Political Warfare activities because of their ability to conduct low visibility, low-footprint operations. USSOCOM will plan, coordinate, and synchronize global SOF support to Political Warfare campaigns with interagency partners, GCCs, TSOCs, and vital partners in the GSN, while the TSOC itself will plan SOF's support to their GCCs theater campaign plan. The implications associated with integrating the various capabilities of special warfare and surgical strike supporting global Political Warfare activities indicate the clear need for a Joint Special Warfare Command.

While by no means seeking to dominate a whole-of-government, civilian-led Political Warfare campaign, SOF will emerge as a key, central element of Political Warfare integration and execution, given its expertise contained in its units manned, trained, and equipped to conduct irregular warfare operations and activities to support Political Warfare objectives. SOF's two critical capabilities, special warfare and surgical strike, provide skill sets instrumental to achieving Political Warfare objectives. SOF can provide scalable force packages ranging from single operators, to small teams, to regimental size forces. SOF can achieve Political Warfare objectives by unilaterally executing operations in a covert or clandestine manner, or through and with indigenous personnel in politically sensitive or hostile environments.

c. Embrace the Human Domain

Successful Political Warfare requires persistent presence and accrued deep understanding, as well as Cognitive Depth and Cognitive Security. These facets of Political Warfare's activities presume an ability to prevail within the Human Domain. Rather than simply operating in the Human Domain or obtaining an experience-based familiarity with specific environments, SOF, its units, and its leader development approaches need to develop and cultivate "a comprehensive discipline to identify, understand, and influence, through word and deed, relevant individuals, groups, and populations." A comprehensive discipline embodied in individual and collective learning, developed concepts, and DOTMLPF derivatives, can elevate Human Domain considerations to the point that they consistently inform the outlining of SOF objectives, actions, and activities.

Rendered formal, a discipline associated with the Human Domain should establish a "common conceptual framework" to generate "comprehension of the elements shaping human decision-making and associated behavior," thus improving environmental understanding throughout a SOF force. Additionally, a formal discipline of Human Domain study, experimentation, and analysis should improve Political Warfare planning

[132] As an example, see U.S. Pacific Command, "Joint Interagency Task Force West," U.S. Pacific Command, accessed July 10, 2014, http://www.pacom.mil/Contact/Directory/JointIntegragencyTaskForceWest.aspx.; The JIATF West Strategy is built on the premise of interagency cooperation. JIATF West partners with U.S. and foreign law enforcement agencies through regional U.S. Embassies and their respective country teams. We also partner with regional law enforcement agencies, such as New Zealand Police, Australian Federal Police, and Australian Customs Service, who coordinate complementary capabilities in the region. We bring military and law enforcement capabilities together to combat and reduce transnational crime in the Asia-Pacific.

and execution through a redefined SOF operational framework that can understand population centric conflicts and can access "culturally-relevant and credible sources of legitimacy to win support and develop partners to their full potential."[133]

5. Conclusion

The U.S. can choose continued leadership in the global struggle against extremism, wanton violence, and the violation of democratic and civilized norms by states and nonstate actors. Put differently, not only does this leadership garner advantages for the American people, but the international arena remains without another state whose national power, values, norms, practices, and legitimacy enable it to fulfill the leadership role that America has shouldered for more than half a century. Rather than any reluctance to preserve global leadership in recent years, America's senior policymakers have affirmed that American leadership must remain "the one constant in an uncertain world."[134]

Yet, the application of national power through large-scale, extended military engagements, or episodic, targeted forays, will not effectively counter or deter the species of threats to the U.S. and her partners characteristic of the FOE. As these threats proliferate during an area of fiscal limitations and diversify as increasingly hybrid, asymmetric, and ambiguous, U.S. leaders require policy options supported by sustainable, integrated strategies able to proactively shape the operating environment or counter adversary hybrid warfare. In order to be sustainable, such strategies need to be affordable and account for likely force structure trends to be integrated, strategy needs to embrace the whole-of-government approach in concept and implementation, including foreign state and nonstate partners whenever it serves U.S. and shared interests.

These requirements necessitate an adoption of political warfare, through the evolving synchronization of associated actions, actors, and theaters of operation. The synchronized whole-of-government application of forms of Unconventional Warfare, in support of Security Sector Assistance, diplomatic engagement, economic measures, and cyber considerations, constitutes the twenty-first-century "employment of all the means at a nation's command, short of war, to achieve its national objectives." Fully engaging "civilian power" while embracing a small-footprint yet enduring forward military presence,[135] Political Warfare is politically, economically, and diplomatically sustainable. Political Warfare also presumes mastery of the Human Domain, in order to understand and influence populations while limiting kinetic actions as much as possible. SOF is Joint Force tool prepared to conduct several Political Warfare activities, and is suited to coordinate the military aspects within the overall whole-of-government approach to extended-duration, small-footprint, and integrated campaigns. Fully employing the contribution of SOF Support to Political Warfare will enable the achievement of National Security objectives in the twenty-first century.

---

[133] USSOCOM, *Operating in the Human Domain* Version 0.70 (5 September 2014), 6-7.

[134] "Weekly Address: America is Leading the World," The White House Blog, 27 Sep 2014: http://www.whitehouse.gov/blog/2014/09/27/weekly-address-america-leading-world.

[135] See Hillary Rodham Clinton, "Leading through Civilian Power: Redefining American Diplomacy and Development," *Foreign Affairs*, November-December 2010: http://www.foreignaffairs.com/articles/66799/hillary-rodham-clinton/leading-through-civilian-power; Department of State & USAID, *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review.*

C. CYBERSECURITY AND OPERATIONS

COMMENTARY

by
Douglas C. Lovelace, Jr.

In Section C of this volume we turn to a major division of hybrid warfare: cyberwarfare. We begin this section by offering a January 5, 2015, Congressional Research Service (CRS) Report on *Cyber Operations in DOD Policy and Plans: Issues for Congress*. Prior volumes in this series have reported on cyberwarfare, but not within the context of hybrid warfare. Additionally, evolving understanding of the threat to U.S. national security from cyberspace, as well as changing attitudes and policies concerning the offensive use of cyberweapons by the United States, warrant periodic reexamination of this area of hybrid warfare.

The CRS report begins appropriately by grounding the reader with a shorthand definition of cyberspace and poses the central question: Is the United States prepared to defend itself from cyber attacks that could cripple critical infrastructure, as well as hamper effective application of military forces to defend the nation and promote its interests? The report correctly observes that the frequency and severity of cyberattacks are on the rise. This is to be anticipated, given the nation's ever-increasing dependence on cyberspace in both the civil and military sectors. Significantly, the report correctly states that U.S. strategy for conducting cyberwarfare requires further development. For example, the rules of engagement for launching offensive cyber operations are still evolving, and discussion continues as to whether the existing body of international law known as the law of armed conflict is sufficient for guiding and adjudicating cyberwarfare operations. The report correctly observes that there is no consensus on what constitutes acts of cyberwar.

The report provides overviews of its topics without getting into technical details. Still the general discussions of the cyber operating environment, the categories of cyber weapons, and the targets on which they may be brought to bear help the reader discern the broad contours of cyberwarfare. To their credit, the report's authors discuss the extraordinarily important issue of attribution of cyberattacks. However, the examination of attribution issues warrants far more detailed analysis. Without confidence that a cyberattack can be attributed to a source with a fairly high degree of confidence, U.S. retaliatory actions are unlikely. This is so for two reasons. First is the adherence by U.S. forces to the rule of war that requires that only belligerents be targeted and civilian collateral damage be minimized, or at least kept proportional to the importance of destroying or negating the belligerent target.. The second, and perhaps more perplexing, reason is that the interconnected nature of the internet and the manner in which the

virtually unfathomable network is exploited to mount cyberattacks makes assessments of potential collateral damage extraordinarily difficult if not impossible in some cases. Adversaries know that by cleverly avoiding attribution, they can hobble U.S. responses and act with relative impunity.

The second document in Section C is an April 22, 2015, Congressional testimony report by the General Accountability Office (GAO) on *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems*. It does not address cyberwarfare directly, but drives a home a point that is central for the defense of U.S. cyber systems. Because of the nature of the internet and the nature of critical U.S. cyber systems that are not connected to the internet but are still vulnerable to cyberattack, the first line of defense is at the level of federal agencies and the users (and contractors) within or associated with those agencies. However, there are competing objectives at the user level. The user's cybersystem architecture must be sufficiently open to afford the exploitation of cyberspace required by the agency to accomplish their missions and perform their functions. At the same time, preventive measures, such as firewalls, must be sufficiently robust to protect the systems from cyberattack. It is this tension that provides adversaries avenues of attack through vulnerable seams. While the GAO report focuses on defensive and remedial measures, one must understand that they, by themselves, are insufficient.

The next document presented in Section C illustrates and elaborates on the points made in *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems*. The June 24, 2015, Congressional testimony report by the GAO on *Cybersecurity: Recent Data Breaches Illustrate Need for Strong Controls Across Federal Agencies*, discusses the specific challenges facing federal agencies, as they attempt to defend against cyberattacks. At the same time, the report shows that cyberattacks show a steep and steadily increasing trend—from 5,503 in 2006 to 67,168 in 2014! However, the increasing frequency of the attacks does not sufficiently describe the magnitude of the threat.

One must also take into account the increasing scale of the attacks and the concomitant increase in potential damage that may result. As the report astutely notes, the June 2015 attack on the U.S. Government's Office of Personnel Management (OPM) compromised the personal information of more than four million current and former federal employees and the OPM has yet to determine the impact of such an unprecedented attack. The Internal Revenue Service (IRS) also reported a successful attack that compromised information on U.S. taxpayers, and the U.S. Postal Service reported a September 2014 cyberattack that compromised the personal information of over 800,000 employees. The frequency and severity trend lines call into question the efficacy of users' defensive measures and suggest that a more comprehensive "provide for the common defense" approach is needed.

We complete Section C with a March 27, 2015, CRS report entitled "Cyberwarfare and Cyberterrorism: In Brief." This short but informative report raises more questions than it answers. It correctly states that there is no international consensus on what type of cyberattack constitutes an act of war. It defines cyberwar very narrowly as state on state conflict. It also draws distinctions between cyberwarfare, cyberterrorism, cybercrime, and cyberespionage, concluding that the distinctions are important in determining appropriate responses. Much of the report's analysis seems overly academic. Distinctions between cyberwarfare, cyberterrorism, cybercrime, and cyberespionage have limited utility in this era of hybrid warfare. All are components and must be viewed holistically. The diversity of documents presented in this section is intended to make that point.

DOCUMENT NO. 5

CYBER OPERATIONS IN DOD POLICY AND PLANS: ISSUES FOR CONGRESS

CRS Report R43848

Catherine A. Theohary
Specialist in National Security Policy and Information Operations

Anne I. Harrington
APSA Congressional Fellow

January 5, 2015

Summary

Cyberspace is defined by the Department of Defense as a global domain consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Attacks in cyberspace have seemingly been on the rise in recent years with a variety of participating actors and methods. As the United States has grown more reliant on information technology and networked critical infrastructure components, many questions arise about whether the nation is properly organized to defend its digital strategic assets. Cyberspace integrates the operation of critical infrastructures, as well as commerce, government, and national security. Because cyberspace transcends geographic boundaries, much of it is outside the reach of U.S. control and influence.

The Department of Homeland Security is the lead federal agency responsible for securing the nation's non-security related digital assets. The Department of Defense also plays a role in defense of cyberspace. The National Military Strategy for Cyberspace Operations instructs DOD to support the DHS, as the lead federal agency, in national incident response and support to other departments and agencies in critical infrastructure and key resources protection. DOD is responsible for defensive operations on its own information networks as well as the sector-specific agency for the defense of the Defense Industrial Base. Multiple strategy documents and directives guide the conduct of military operations in cyberspace, sometimes referred to as cyberwarfare, as well as

the delineation of roles and responsibilities for national cybersecurity. Nonetheless, the overarching defense strategy for securing cyberspace is vague and evolving.

This report presents an overview of the threat landscape in cyberspace, including the types of offensive weapons available, the targets they are designed to attack, and the types of actors carrying out the attacks. It presents a picture of what kinds of offensive and defensive tools exist and a brief overview of recent attacks. The report then describes the current status of U.S. capabilities, and the national and international authorities under which the U.S. Department of Defense carries out cyber operations. Of particular interest for policy makers are questions raised by the tension between legal authorities codified at 10 U.S.C., which authorizes U.S. Cyber Command to initiate computer network attacks, and those stated at 50 U.S.C., which enables the National Security Agency to manipulate and extrapolate intelligence data—a tension that Presidential Policy Directive 20 on U.S. Cyber Operations Policy manages by clarifying the Pentagon's rules of engagement for cyberspace. With the task of defending the nation from cyberattack, the lines of command, jurisdiction, and authorities may be blurred as they apply to offensive and defensive cyberspace operations. A closely related issue is whether U.S. Cyber Command should remain a sub-unified command under U.S. Strategic Command that shares assets and its commander with the NSA. Additionally, the unique nature of cyberspace raises new jurisdictional issues as U.S. Cyber Command organizes, trains, and equips its forces to protect the networks that undergird critical infrastructure. International law governing cyberspace operations is evolving, and may have gaps for determining the rules of cyberwarfare, what constitutes an "armed attack" or "use of force" in cyberspace, and what treaty obligations may be invoked.

Introduction[1]

Cyberspace has taken on increased strategic importance as states have begun to think of it as yet another domain—similar to land, sea, and air—that must be secured to protect their national interests. Cyberspace is another dimension, with the potential for both cooperation and conflict. The Obama Administration's 2010 National Security Strategy identifies cybersecurity threats "as one of the most serious national security, public safety, and economic challenges."

Cyberattacks are now a common element of international conflict, both on their own and in conjunction with broader military operations. Targets have included government networks, media outlets, banking services, and critical infrastructure. The effects and implications of such attacks may be small or large; cyberattacks have defaced websites, temporarily shut down networks and cut off access to essential information and services, and damaged industrial infrastructure. Despite being relatively common, cyberattacks are difficult to identify at their source and thwart, in particular because politically motivated attacks are often crowd-sourced,[2] and online criminal organizations are easy to join. Suspicions of state-sponsored cyberattacks are often strong but

[1] Information contained in this report is derived from unclassified open source material and discussions with senior government officials and industry technology and security experts.

[2] Crowd-sourcing refers to the use of online communities to obtain ideas, information, and services.

difficult to prove. The relative anonymity under which actors operate in cyberspace affords a degree of plausible deniability.

This report focuses specifically on cyberattacks as an element of warfare, separate and distinct from diplomatic or industrial espionage, financially motivated cybercrime, or state-based intimidation of domestic political activists.[3] However, drawing clean lines between cyberwar, cyberterrorism, cyberespionage, and cybercrime is difficult. State and non-state actors carry out cyberattacks every day. When and under what conditions cyberattacks rise to the level of cyberwar is an open question. Some experts contend that all warfare, including cyberwarfare, by definition includes the destruction of physical objects. According to this point of view, to be an act of cyberwarfare, the attack must originate in cyberspace and result in the destruction of critical infrastructure, military command-and-control capabilities, and/or the injury or death of individuals.[4] On the other hand, some analysts have a more inclusive view of cyberwarfare. These experts would include, in addition to cyberattacks with kinetic effects, the exfiltration or corruption of data, the disruption of services, and/or manipulation of victims through distraction.

As our military becomes increasingly information dependent, potential vulnerabilities in network-centric operations are crystalized. A cyberattack on a military asset may be considered an act of war to which the military will respond under the Law of Armed Conflict. However, there may also be attacks on civilian systems which would warrant a military response.

Background

Cyberspace: The Operating Environment

The Internet represents a portion of the global domain of cyberspace; however, there are networks and systems that are not connected to the Internet. Included among these are national strategic assets whose compromise could have serious consequences. In its 2010 Quadrennial Defense Review, the Department of Defense (DOD) identified cyberspace as a global commons or domain, along with air, sea and space. Previous views of cyberspace had focused mainly on the enabling or force multiplier aspects of information technology and networked workfare. Cyberspace is currently defined by the DOD as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[5] It is also described in terms of three layers: (1) a physical network, (2) a logical network, and a (3) cyber-persona:[6]

- The *physical network* is composed of the geographic and physical network components.

[3] Industrial espionage events are widely covered and notorious: attacks on Target, Home Depot, and Sony have caught national attention and have serious economic implications. Such events, however challenging, are not considered warfare for purposes of this report.

[4] Bruce Schneier, *Schneier on Security* (Indianapolis: Wiley, 2008); Michael Schmitt et al., *Tallinn Manual on the Internationl Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge: Cambridge University Press, 2013.

[5] Department of Defense Joint Publication 3-12, *Cyberspace Operations*, February 5, 2013.

[6] Ibid.

- The *logical network* consists of related elements abstracted from the physical network, (e.g., a website that is hosted on servers in multiple locations but accessed through a single URL).
- The *cyber-persona layer* uses the rules of the logical network layer to develop a digital representation of an individual or entity identity.

Because one individual or entity can have multiple cyber personae, and vice versa, attributing responsibility and targeting attacks in cyberspace is challenging. Another challenge lies in insider threats, when an authorized user or users exploits legitimate access to a network for nefarious purposes.

From a military perspective, the *operational environment* is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.[7] The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information, further broken down into the physical, informational, and cognitive dimensions.

Cyberspace operations employ capabilities whose primary purpose is to achieve objectives in or through cyberspace. The following section gives examples of some of the tools through which these objectives may be achieved.

Cyber Weapons

There are several tools through which effects in cyberspace are achieved. Effects can range in severity from disrupting or slowing down access to online goods and services, to degrading and destroying entire network operations. The actors who employ these tools can range from individual hacker groups to nation states and their proxies. The following section describes the most common attack tools, or cyber weapons, that these actors employ.

Malware

Malware is a general term for malicious software. Bots, viruses, and worms are varieties of malware. Bots, as described below, are used to establish communication channels among personal computers, linking them together into botnets that can be controlled remotely. Botnets are one way that other forms of malware, such as viruses and worms, spread. As the names imply, viruses spread by infecting a host. They attach themselves to a program or document. In contrast, worms are stand alone, self-replicating programs.[8]

The first known malware aimed at PCs, a virus, was coded in 1986 by two brothers in Pakistan. They named the virus Brain after their computer shop in Lahore and included their names, addresses, and phone numbers in the code. Calling Brain malware is slightly misleading because the brothers had no ill intentions. They were simply curious to find out how far their creation could travel. Within a year it had traveled around the globe.[9]

[7] Ibid.

[8] CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

[9] Joshua Davis, "John McAfee Fled to Belize, But He Couldn't Escape Himself," *Wired*, December 24, 2012, http://www.wired.com/2012/12/ff-john-mcafees-last-stand/all.

Malware that targets the internal networks of particular companies are often spread by infecting "watering-holes," a term for public websites frequented by employees. Another common method is "spearphishing"—sending emails to targeted individuals that contain malicious links. The email appears to be innocuous and sent from a trusted source, but clicking on the link opens a virtual door to outsiders.[10] So-called "air-gapped" networks, computer systems that are not connected to the Internet, are not vulnerable to these types of attacks; however, such networks can be infected by viruses and worms when an external device, such as a thumb drive, is inserted into a networked computer.

Botnets

Robotic networks, commonly known as botnets, are chains of home and business PCs linked together by a script or program. That program (the bot) enables a single operator to command all of the linked machines. Botnets are not necessarily malicious. The computer code botnets use also enables desirable communication across the Internet, such as the chat rooms that were popular in the 1990s. However, programmers have figured out how to exploit vulnerabilities in widely used Microsoft Windows operating platforms to degrade, destroy, and manipulate computer networks—often without the knowledge of the machine's owner or local operator.[11] Because they are automated programs, when released, bots lurk on the Internet and take over computers, turning them into a network of "zombies" that can be operated remotely. The majority of email spam is generated by botnets without the host computer's knowledge.[12] In fact, owners are often not aware that their computers are part of a botnet, the only indication of which is sluggish response time.[13]

Early botnet operators were often skilled coders. In contrast, today an underground industry of skilled botnet providers exists, but operators no longer have to be fluent coders. Starting in 2004, bots got considerably easier to use as the result of new applications that allowed hackers to build bots by pointing and clicking, resulting in a bloom of spam in email inboxes across the globe.[14] In addition to unwanted advertising, botnets can generate denial-of-service (DoS) attacks and spread malware.

Distributed Denial of Service Attacks

Distributed Denial of Service (DDoS) attacks flood their target with requests, consuming the target's bandwidth and/or overloading the capacity of the host server, resulting in service outages. These attacks are "distributed" because effective attacks employ

[10] Chris Strohm, "Hedge-Fund Hack Part of Wall Street Siege Seen by Cyber-Experts," *BloombergGovernment*, June 23, 2014.

[11] Zheng Bu, Pedro Bueno, Rahul Kashyap, et al., *The New Era of Botnets*, McAfee: An Intel Company, white paper, Santa Clara, CA, 2010, pp. 3-4, http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf.

[12] John Markoff, "A Robot Network Seeks to Enlist Your Computer," *New York Times*, October 20, 2008.

[13] Richard A. Clark and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), p. 13.

[14] Zheng Bu, Pedro Bueno, Rahul Kashyap, et al., *The New Era of Botnets*, McAfee: An Intel Company, White Paper, Santa Clara, CA, 2010, pp. 3-4, http://www.mcafee.com/us/resources/white-papers/wp-new-era-of-botnets.pdf.

botnets, distributing the source of requests across an entire network of zombie computers. DDoS attacks are unique for three reasons: (1) they exploit vulnerabilities in their target's software or operating system that cannot be easily repaired or "patched;" (2) each individual packet is a legitimate request—only the rate and total volume of packets gives an attack its destructive impact; and (3) the severity of the attack is measured in terms of its duration. Unlike malware, which alters or infects its target, DDoS attacks consist of the same types of packets, a unit of data, that a typical user would send when making a legitimate request. The only difference is in the number and frequency with which the attacker generates requests. The goal of a DDoS attack is to render targeted networks unavailable or non-responsive, thereby preventing users from accessing information for the duration of the attack.[15]

The pathway of a DDoS attack is known as a *vector*. Today it is common for an attack to have multiple vectors. A DDoS attack carried out by botnets along multiple vectors can interrupt services for days, weeks, or even months. More sophisticated attacks take advantage of vectors that amplify their strength through a process that generates exponential reverberations. The ability to amplify an attack, for instance by tricking a server into responding to a target with an even larger packet than what was originally sent, increases an already substantial asymmetric advantage. Botnet applications not only make DDoS attacks relatively easy to mount, but the redundant and decentralized nature of the Internet makes attribution difficult.[16] In theory, a DDoS attack could temporarily take down the entire web by simultaneously targeting the 13 root servers on which all Internet traffic depends.[17] In practice, this has not yet happened.

Automated Defense Systems

Retaliatory hacking, a response to network breaches that has been used in the private sector, has gained traction within DOD as a means to stage an "active defense." These potentially offensive operations may occur when a systems administrator sees an intrusion and in turn breaches the assumed point of origin, either to retrieve or destroy information. However, such activities are complicated for two reasons: uncertainty in attack attribution and active defense may violate terms enacted in the Computer Fraud and Abuse Act of 1986.[18] This law criminalizes unauthorized breaches and other computer-related activity, including the distribution of malware and use of botnets. Although the military would be involved in a counterattack only during a national security crisis, the government may tacitly encourage companies to engage in retaliatory hacking as the first line of defense for the nation's critical infrastructure. For example, the Defense Advanced Research Projects Agency (DARPA) has launched a Cyber Grand Challenge program to hasten the development of automated security systems capable of responding to and neutralizing cyberattacks as fast as they are launched. Automated defense

[15] Ziv Gadot, Eyal Benishti, Lior Rozen, et al., *Radware Global Application & Network Security Report 2012*, Radware, White Paper, Mahwah, NJ, 2013, p. 1, file:///C:/Users/aharrington/Downloads/a7b991da-b96e-4cd7-bf8c-236b1e7e4c67.pdf.

[16] Ziv Gadot, Eyal Benishti, Lior Rozen, et al., *Radware Global Application & Network Security Report 2012*, Radware, white paper, Mahwah, NJ, 2013, p. 18.

[17] http://www.root-servers.org/.

[18] 18 U.S.C. §1030.

systems may also be configured to launch a counterattack in the direction of a network breach.

Targets

Attacks on information technology destroy, degrade, and/or exfiltrate data from a host computer. The intended effect of a cyberattack can be related to the attack target. Within the context of cyberwarfare, two areas are attractive targets for a potential adversary: government and military networks, and critical infrastructure and industrial control systems.

Government and Military Networks

Nation states and other entities target government and military networks to exfiltrate data, thereby gaining an intelligence advantage, or to potentially plant a malicious code that could be activated in a time of crisis to disrupt, degrade, or deny operations. In 2008, The Pentagon itself was a target of a massive breach, when an infected thumb drive was inserted into a computer connected to DOD classified networks. The discovery of the malware, named Agent.btz, led to a massive cleanup operation code-named Buckshot Yankee.[19] While the incident appeared to be related to espionage and theft of sensitive information, it is possible that malware could also contain a hidden, more nefarious function, such as the capability to disable communications or spread disinformation.

Critical Infrastructure and Industrial Control Systems

Civilian critical infrastructure comprises networks and services that are considered vital to a nation's operations and are owned and operated by the private sector.[20] Examples of these sectors include energy, transportation, financial services, food supplies, and communications. These sectors may be particularly vulnerable to cyberattack because they rely on open-source software or hardware, third-party utilities, and interconnected networks.

Large-scale industrial control systems (ICS), such as the supervisory control and data acquisition (SCADA) systems that provide real-time information to remote operators, present a unique vulnerability. Disabling an electric power plant by attacking its SCADA system, for instance, will have many follow-on effects. These systems, as they control the operations of a particular platform, are referred to by the Defense Department as "operations technology."

From highly specialized equipment, such as uranium enrichment plants, to mundane heating and air conditioning systems and office photocopiers, the capability to remotely control industrial hardware for maintenance and operations purposes also makes these machines vulnerable to cyberattacks. Attacks against operations technology (OT) are

[19] Ellen Nakashima, "Cyber-intruder sparks response, debate" *Washington Post*, December 8, 2011, http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html.

[20] Critical Infrastructure is defined in 42 U.S.C. 5195c(e) as: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

different than information technology (IT) attacks because OT attacks can produce kinetic effects. Although OT controls primarily mundane infrastructure, these built environments are increasingly networked environments, which adds a complicated layer to training and maintenance.

Actors and Attribution

With low barriers to entry, multiple actors may take part in use of the Internet and networked technology as a means to achieve strategic effects. These actors may represent nation states, politically motivated hacker groups or "hactivists," or terrorist and other criminal organizations. Directly attributing a cyberattack to any one of these groups can be challenging, particularly as they may sometimes operate in concert with each other, though for differing motivations.

Nation States

Cyberwarriors are agents or quasi-agents of nation states who develop capabilities and undertake cyberattacks to support a country's strategic objectives.[21] These entities may or may not be acting on behalf of the government with respect to target selection, attack timing, or type(s) of cyberattack. Moreover, cyberwarriors are often blamed by the host country when the nation that has been attacked levies accusations against that country. Typically, when a foreign government is presented with evidence that a cyberattack is emanating from its country, the nation that has been attacked is told that the perpetrators acted of their own volition, not at the behest of the government.

Politically Motivated Hacktivists

Cyberhactivists are individuals who perform cyberattacks for pleasure, or for philosophical or other nonmonetary reasons. Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker), and a "hacktivist," such as a member of the cybergroup Anonymous, who undertakes an attack for political reasons. The activities of these groups can range from simple nuisance-related DoS attacks to disrupting government and private corporation business processes.

Terrorists and Organized Crime

Cyberterrorists are state-sponsored or non-state actors who engage in cyberattacks as a form of warfare. Transnational terrorist organizations, insurgents, and jihadists have used the Internet as a tool for planning attacks, recruiting and radicalizing members, distributing propaganda, and communicating.[22] No unclassified reports have been published regarding a terrorist-initiated cyberattack on U.S. critical infrastructure. However, the essential components of that infrastructure are demonstrably vulnerable to access and even destruction via the Internet. In 2007, a U.S. Department of Energy

[21] For additional information, see CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

[22] For additional background information, see archived CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson.

test at Idaho Labs demonstrated the ability of a cyberattack to shut down parts of the electrical grid. In the test, known as the Aurora Experiment, a cyberattack on a replica of a power plant's generator caused it to self-destruct.

Advanced Persistent Threats

The term "Advanced Persistent Threat" (APT) has been used within the intelligence community to describe nation-state cyberespionage activities. However, organizations that may or may not be state-sponsored may also use APT techniques to gain a competitive military advantage. Characteristics of an APT include a high level of sophistication in the malware's code, along with the targeting of certain networks or servers to glean specific information of value to the attackers or to cause damage to a specific target. Likely targets include government agencies and corporations in critical infrastructure sectors such as financial, defense, information technology, transportation, and health. In 2013, the U.S. security firm Mandiant published a 60-page intelligence report on a Chinese operation, which the firm identified as APT1, that allegedly stole hundreds of terabytes of data from at least 141 organizations across 20 industries worldwide since 2006.[23] Mandiant's analysis concluded that APT1 is likely government-sponsored (believed to be the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department) and one of the most persistent of China's cyber threat actors.

Attribution Issues

Analysts trying to determine the origin of a cyberattack are often stymied by the use of botnets. First, computers infected by a botnet may be located in countries around the world, obscuring the country of origin of the botnet's commander, known as the bot herder. Second, the identity of the server controlling the botnet may be obscured by the prevalence of peer-to-peer software[24]. In addition to these concerns, Internet provider (IP) addresses that might otherwise trace the location of a computer that launched an attack can be faked (known as "spoofing"), and even with a valid IP address, it may be virtually impossible to verify who was behind the computer at the time an attack was launched. This uncertainty is also true of a computer that has been infected unbeknownst to the user. At the nation-state level, a certain amount of deniability in terms of cybersecurity and network control is plausible. Given the proliferation of hacker organizations and the cyber weapons at their disposal, states can easily claim a lack of responsibility for rogue cyber actors and attacks that appear to stem from within state borders.

Threat Environment

Cyberattack is a persistent threat. This section describes events that have provoked a political and/or military response from leaders in one or more state. The case studies provided are not exhaustive; excluded are many instances of cyber espionage that could arguably be considered international incidents. Instead, this section focuses primarily on cyberattacks that (1) have had strategic effects, (2) play a tactical role in a larger military operation, (3) carry implications for the ability of a state to carry out future military

[23] Accessed at http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[24] Peer-to-peer software refers to computer networks in which each computer can act as a server for the others, obviating the need for a central server for command and control.

operations, or (4) threaten public trust in the reliability and security of information on the Internet.

Cyberattack Case Studies

Each of the cyberattacks in this section illustrates a different tactical and/or strategic use of weapons in cyberspace. The events in each of these cases raised questions about acts of terror and/or war in cyberspace and the role of the military.

Estonia: Cyberattack as Siege

Estonia is a Baltic state of approximately 1.3 million people that regained its independence from the Soviet Union in 1991. In 2004, Estonia joined the European Union (EU). Technologically, Estonia distinguished itself as the home of Skype, a widely popular online voice and video communication software. Today, Estonia is one of the most wired nations on earth. Estonians conduct most of their daily business online, even carrying out the basic rights and responsibilities of democratic citizenship, such as voting, through the Internet. As a result, Estonia is particularly vulnerable to cyberattack.[25]

On the morning of April 28, 2007, waves of DDoS attacks besieged websites in Estonia. Over the next two weeks, attackers targeted crucial sectors, shutting down Internet access to hundreds of key government, banking, and media web pages. Estonians were unable to bank online or retrieve cash from ATMs. Attackers also targeted Internet addresses for servers, threatening the telephone network and the credit card verification system. Vital services simply ceased to function, unable to stand back up before the next wave of attack. Where possible, organizations cut off all international traffic, closing the gates against the attack. Unlike previous DoS attacks that hit a single site over the course of days, this attack brought communication and commerce in a sovereign nation to a halt for weeks.[26]

The 2007 cyberattacks appear to have originated in Russia. On April 27, 2007, Estonian officials carried out a controversial plan to relocate a World War II-era statue of a Red Army soldier from a central location in Tallinn, the nation's capital, to a military cemetery in a suburb. Despite ominous warnings from the Russian government that removing the statue honoring the sacrifice of Russian soldiers would prove "disastrous for Estonians," Estonia, after 16 years of independence, decided to move the reminder of Soviet occupation.[27]

What role, if any, the Russian government actually played in the attack is unclear. The Russian government claimed the attack was an online version of an angry mob. Evidence suggests that patriotic hackers played an important role in the attack. The Pro-Putin movement Nashi ("Ours"), which organizes political events for young adults, claimed at least partial responsibility for engaging in cyber activities to counter "anti-Fatherland"

[25] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[26] Richard A. Clark and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010).

[27] Ibid.

forces.[28] Suspicion remains about government involvement, though. Patriotic hacking can provide cover for behind-the-scenes coordination efforts.

The attacks followed instructions posted in Russian language Internet chat rooms on how to generate DoS attacks. The posts included calls for a coordinated attack at the stroke of midnight on May 9, the day Russians celebrate their World War II victory. At exactly midnight in Moscow, 11p.m. in Tallinn, nearly 1 million computers around the globe navigated to Estonian websites. Surging at 4 million packets per second, Internet traffic in Estonia increased 200-fold, squeezing the bandwidth of an entire nation.[29]

Prepared for the surge, the head of the Estonian computer emergency response team enlisted the help of individuals responsible for the health and care of the Internet root server system to follow attacks back to their source and block specific computers from accessing the servers. This strategy mitigated the effects of the attack. Then suddenly the surges in traffic stopped as suddenly as they had started.[30]

Because Estonia is a member of NATO and the European Union, this event exposed how unprepared those organizations may have been to respond to a cyberattack against a member state. Had Estonia invoked NATO's Article V collective security provision, doing so would have raised several thorny questions about what kind of attack triggers those alliance obligations. The fact that the cyberattack was targeted at a member state and prompted an official state response was complicated by the inability to identify the aggressor. Moreover, the attack did no physical damage, and in the end did no permanent damage to Estonia's web-based infrastructure. The damage was measurable only in terms of short-lived commercial losses.[31] This kind of cyberattack is sometimes likened to a weather event. Snow storms, although a temporary crisis, rarely have any lasting effects. How serious a threat the storm presents depends, at least in part, on one's capability to weather the storm.[32] Although Estonian Defense Ministers viewed this event in terms of a national security crisis, other security analysts described it as a "cyber riot" or "costly nuisance," comparing it to an electronic sit-in where traffic to public and commercial sites is slowed or blocked to make a political point.

Georgia: Cyberattack and Invasion

In 2008, Russia invaded Georgia by land and air and blockaded the nation by sea. Simultaneously, pro-Russian hackers besieged Georgia's Internet, all but locking down communication for the duration of the armed conflict. Although Georgia is not a heavily wired society—at the time experts ranked it 74th out of 234 nations in terms of Internet addresses, behind Nigeria, Bangladesh, Bolivia, and El Salvador[33]—the attacks were a

[28] Peter Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2013), pp. 110-111.

[29] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[30] Ibid.

[31] Ibid.

[32] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Washington, DC: RAND, 2007).

[33] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

significant event in the development of cyberwar because they synchronized patriotic hacking with government-sponsored military movements.[34]

Like Estonia, Georgia is a former Soviet state; it declared its independence in 1991. Tensions with Russia have persisted and were not eased by Georgia's failed bid to join NATO in the spring of 2008.[35] Over the course of that same summer, well-armed Russian-backed separatists began consolidating control over two predominately Russian-speaking regions on the country's northern border, Abkhazia and South Ossetia. As tensions rose, separatists—some of whom were believed to be Russian special forces—clashed with Georgian police.[36]

In mid-July, the cyberattacks started. The Georgian President's website was the first high-profile target. Although the DDoS attack vector passed through a U.S.-based, commercial IP address, experts identified the malware that hackers used to generate the attack as a "MachBot" DDoS controller. Machbot is written in Russian and a known tool of Russian criminal groups.[37] Reportedly, pro-Russian hackers were discussing the attacks on websites and in chat rooms; in addition to the higher-profile attack, hackers also temporarily shut down Georgian servers.[38]

Three weeks later, on August 8, Russian tanks crossed the border into South Ossetia. Accompanying the ground invasion was a second round of DDoS attacks. One of the first targets was an online forum popular with pro-Georgian hackers. This preemptive attack reduced, but did not entirely eliminate, the number of counterattacks against Russian targets.[39] As the troops moved in, Georgians were unable to access 54 local websites with critical information related to communications, finance, and the government.[40]

Georgian officials transferred critical Internet resources to U.S., Estonian, and Polish host servers. Refuge for some websites, including those of the President and Ministry of Defense, was granted by an American executive from the privately owned web-hosting company Tulip Systems, but without the knowledge or authority of the U.S. government. Tulip Systems reported experiencing attacks on its servers, a fact that raises troubling questions about sovereignty in the age of cyberwarfare.[41]

The fighting lasted five days. During that time, Georgia's Internet connection was besieged by attacks and unable to communicate via web with the media. Reportedly, cyberattacks followed the same target patterns as the land and air invasions, with DDoS attacks taking out the communications prior to bombing or ground troop movements.

---

[34] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011.

[35] For further discussion, see CRS Report RL34618, *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests*, by Jim Nichol.

[36] Mikheil Saakashvili, "Let Georgia be a lesson for what will happen to Ukraine," *The Guardian*, March 14, 2014.

[37] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008, p. 65, http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/08winter/korns.pdf.

[38] David Hollis, "Cyberwar Case Study: Georgia 2008 " *Small Wars Journal*, January 6, 2011, p. 3.

[39] Ibid.

[40] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, p. 2.

[41] Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," Parameters, Winter 2008, p. 65, http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/08winter/korns.pdf.

Perhaps most importantly, the cyberattacks and the air attack spared critical infrastructure associated with Georgia's energy sector.[42]

Iran: Cyberattack with Kinetic Effect

When programmers at a small Belarussian cybersecurity firm first discovered a new computer worm in June 2010, they knew it was unusually sophisticated because it was exploiting a "zero-day vulnerability" in Microsoft Windows. Malware that outsmarts programmers and developers by identifying an unanticipated weakness in the Windows operating systems is rare. Even so, the cybersecurity specialists who originally detected Stuxnet had no idea just how sophisticated this new worm would turn out to be.[43] The idea of sabotaging industrial control systems from a remote location was not new, but creating a worm that could search for a single target was revolutionary, and this is what Stuxnet's authors had achieved.[44]

The intended target appears to have been industrial control systems in Iran's nuclear facility at Natanz. The first clue was the pattern of infected computers: the Stuxnet worm attacked air-gapped networks (i.e., those not connected to the Internet). The worm propagated by infecting local hosts via a USB thumb drive. While a computer scanned the contents of the inserted thumb drive, the worm surreptitiously installed a partially encrypted file. This file contained a stolen security certificate that fooled its host into believing that the Stuxnet worm was a trusted program. From its initial host computer, Stuxnet could travel throughout a networked system. Although Stuxnet did not propagate itself through the web, if an infected computer was connected to the Internet, the worm would automatically begin sending information back to one of two domain names hosted on servers in Denmark and Malaysia. Once cybersecurity experts realized that infected computers were "phoning home," they redirected that traffic into a sinkhole they controlled. By analyzing the collected data, the experts were able to map the pattern of infection. Unlike most malware, which spreads rapidly through densely networked countries like the United States and South Korea, Stuxnet was overwhelmingly concentrated in Iran. Of the first 38,000 infected computers, 22,000 were located in Iran.[45]

---

[42] David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, p. 4.

[43] P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[44] In his memoir, Thomas Reed, a former U.S. Air Force secretary who served in the National Security Council during President Reagan's tenure, describes a successful CIA plot to sabotage the Soviet Union's Siberian pipeline in 1982 by tricking Moscow into stealing booby-trapped software. The faulty ICS software overpressurized the system causing "the most monumental non-nuclear explosion and fire ever seen from space." Alec Russell, "CIA plot led to huge blast in Siberian gas pipeline" *The Telegraph*, February 28, 2004, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html; Michael Joseph Gross, "A Declaration of Cyber-War," *Wired*, April 2011, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

[45] Eventually, specialists identified over 100, 000 corrupted devices. For more see P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/; Ralph Langer, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," November, 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf; William J. Broad, John Markoff, and David Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0; Paul Kerr, John Rollins and Catherine Theohary, "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability," *Congressional Research Service Report*, December 9, 2010.

The second clue as to Stuxnet's intended target was that, reportedly starting in 2009, International Atomic Energy Agency inspectors noticed the significantly higher-than-average rate at which Iran was removing and repairing centrifuges in its uranium enrichment facility at Natanz.[46] Centrifuges built to process natural uranium into a form capable of fueling a nuclear power plant, or building a nuclear warhead, are extremely delicate. Among the fastest spinning objects on earth, any irregularities in a centrifuge's rotor will cause imbalances. Even a fingerprint on the rotor would cause it to spin out of control and do irreparable damage.[47] As cybersecurity specialists dug deeper into the code, they identified commands that were specific to the industrial control system Simatic WinCC Step7, produced by the German company Siemens. This is the same controller Iran uses in its uranium-enrichment facilities to control its centrifuges. Once Stuxnet identified its target, the malware automatically commanded the centrifuges to spin at frequencies significantly faster and then slower than normal, doing damage to the delicate rotors. Meanwhile, Stuxnet evaded detection by making it appear to the operators monitoring the system (via a computer screen) that nothing had changed.[48]

The overall effect of Stuxnet on the Iranian nuclear program is unclear. Iran has since acknowledged the attack but maintains that Stuxnet did not change the rate at which it was able to increase its stockpile of enriched uranium.[49] David Albright and Christina Walrond of the Institute for Science and International Security argue that although the rate of production has not changed, starting in late 2009, Iran required more centrifuges to perform the same amount of work. Albright and Walrond did not definitively argue that Stuxnet caused Iran's efficiency to decline, nor did they discount that possibility, instead stating, "It is likely that multiple factors have played a role in the diminished effectiveness of the FEP [fuel enrichment plant]. . . . The available data are too general to determine the actual situation."[50]

No one has claimed responsibility for the attack, but in January 2011, but the *New York Times* reported that Stuxnet was a joint venture of the United States and Israel. Reportedly, Israel constructed a centrifuge plant at Dimona identical to the one in Natanz to simulate the attack. The United States allegedly provided information about

[46] P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[47] Anne Harrington and Matthias Englert, "How Much is Enough? The Politics of Technology and Weaponless Nuclear Deterrence" in *International Relations and the Global Politics of Science and Technology*, eds. Mariana Carpes and Maximilian Mayer, Berlin: Springer, 2014.

[48] The cybersecurity company Symantec has since established that there were multiple variants of Stuxnet. The earlier variant closed valves, causing a build-up of pressure that will make the centrifuge wobble and damage the rotors, rather than directly affecting the rate at which the centrifuge spins. For more, see Institute for Science and International Security, *Basic Attack Strategy of Stuxnet 0.5 rev. 1*, Institute for Science and International Security, Washington, DC, February 28, 2013, http://isis-online.org/isis-reports/detail/basic-attack-strategy-of-stuxnet-0.5/.

[49] Dr. Fereydoun Abassi, Vice President of the Islamic Republic of Iran and Head of Atomic Energy Organization of Iran, "Statement at the IAEA 56th General Conference," September 17, 2012; P. Mittal, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired*, July 11, 2011, pp. http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/all/.

[50] David Albright and Christina Walrond, *Performance of the IR-1 Centrifuge at Natanz*, Institute for Science and International Security, Washington, DC, October 18, 2011, http://isis-online.org/isis-reports/detail/test1/8.

vulnerabilities in the Siemens controller, access to which had been gained through a cybersecurity collaboration between Siemens and the Idaho National Lab.[51]

The DOD and U.S. Cyber Command

The Department of Defense is responsible for securing its own networks, the Department of Defense information networks (DODIN), or .mil domain, formerly known as the Global Information Grid (GIG). The requested cybersecurity budget for DOD was approximately $5.1 billion for FY2015.This figure represents a portion of the President's requested overall IT budget for DOD that same year (approximately $36 billion). The DOD cybersecurity budget grew by $1 billion from 2013 to 2014, but this increase may reflect changes in how DOD programmatic elements have defined "cybersecurity" programs. In general, the DOD cybersecurity budget comprises the following activities: Information Assurance, Cyberspace Operations, National Cybersecurity Initiative/ Defense Industrial Base/Defense Cyber Crime Center, and U.S. Cyber Command.[52]

After recognizing that cyberspace is a global operating domain as well as a strategic national asset, DOD reorganized its cyber resources and established the U.S. Cyber Command in 2010. This sub-unified command under the U.S. Strategic Command is co-located at Fort Meade, Maryland with the National Security Agency (NSA). It combines offensive and defensive capabilities and is commanded by a four-star general, also the director of the NSA. The NSA's primary missions are information assurance for National Security Systems and signals intelligence. Also located within NSA is the Central Security Service, the military's cryptology component. As an intelligence agency, NSA operates under the authorities of Title 50 U.S.C., War and National Defense. U.S. Cyber Command operates under U.S.C. Title 10, Armed Forces—the authorities through which the military organizes, trains, and equips its forces in defense of the nation.

Cyber Command Mission and Force Structure

As previously stated, one of the main missions of U.S Cyber Command is to defend and operate the DODIN. In his nomination hearing before the Senate Armed Services Committee, then-Vice Admiral Michael S. Rogers, tapped to become the head of U.S. Cyber Command, described the duties of the Cyber Commander thusly:

> The Commander, U. S. Cyber Command (USCYBERCOM) is responsible for executing the cyberspace missions specified in Section 18.d.(3)of the Unified Command Plan (UCP) as delegated by the Commander, U.S. Strategic Command (USSTRATCOM) to secure our nation's freedom of action in cyberspace and to help mitigate risks to our national security resulting from America's growing dependence on cyberspace. Subject to such delegation and in coordination with mission partners, specific missions include: directing DODIN operations, securing and defending the DODIN; maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared

[51] William J. Broad, John Markoff, and David Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times,* January 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html? pagewanted=all&_r=0.

[52] Source: Internal Department of Defense budget documents.

> situational awareness of cyberspace operations, including indications and warning; integrating and synchronizing of cyberspace operations with combatant commands and other appropriate U.S. Government agencies tasked with defending the our nation's interests in cyberspace; provide support to civil authorities and international partners. All these efforts support DoD's overall missions in cyberspace of defending the nation against cyber attacks, supporting the combatant commands, and defending Department of Defense networks.[53]

Operators at the U.S. Cyber Command are sometimes referred to as "cyber warriors," although this term does not appear in official Department of Defense definitions. Reports of USCYBERCOM-planned workforce structures yield clues regarding the activities a so-called cyber warrior might undertake. First reported in the *Washington Post*, "The plan calls for the creation of three types of Cyber Mission Forces under the Cyber Command: 'national mission forces' to protect computer systems that undergird electrical grids, power plants and other infrastructure deemed critical to national and economic security; 'combat mission forces' to help commanders abroad plan and execute attacks or other offensive operations; and 'cyber protection forces' to fortify the Defense Department's networks."[54]

These multiservice Cyber Mission Forces numbered under 1,000 in 2013, when DOD announced plans to expand them to roughly 5,000 soldiers and civilians. The target number has since grown to 6,200, with a deadline at the end of FY2016. In early November 2014, a leaked classified document was reported to have stated that "additional capability may be needed for both surge capacity for the [Cyber Mission Forces] and to provide unique and specialized capabilities" for a whole-of-government and nation approach to security in cyberspace.[55] USCYBERCOM Commander Admiral Michael S. Rogers has said that overall, Cyber Mission Forces will be about 80% military and 20% civilian. At a recent conference, Deputy Commander of USCYBERCOM Lieutenant General James McLaughlin said the Cyber Mission Force was being formed into 133 teams of tactical units that will[56] support all Combatant Commands, and that at least half of these teams would be used for defensive measures.

Each of the four military services provides cyber mission forces to USCYBERCOM. All of the services' cyber divisions plan to steadily increase their number of cyber operators over the next two years.

USCYBERCOM and Information Sharing

In May 2011, DOD launched a pilot voluntary program (the DIB Cyber Pilot) involving several defense industry partners, the NSA and DOD, to share classified threat-vector information among stakeholders. Under the DIB Cyber Pilot, NSA shares threat signatures with participating defense companies. One aspect of the program was sharing

[53] Advanced Questions for Vice Admiral Michael S. Rogers, Nominee for Commander, United States Cyber Command, Senate Armed Services Hearing of March 11, 2014, http://www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf.

[54] From http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

[55] http://www.defensenews.com/article/20141103/TRAINING/311030018/As-cyber-force-grows-manpower-details-emerge.

[56] Wyatt Olson, "Cyber Command trying to get running start, add staff," *Stars and Stripes*, December 11, 2014.

by the NSA of threat signatures obtained through its computer monitoring activities. DHS subsequently initiated the Joint Cybersecurity Services Pilot (JCSP) in January 2012 and announced in July that the program would be made permanent, with the renamed DIB Enhanced Cybersecurity Services (DECS) as the first phase. In this program, DHS communicates with participating commercial Internet service providers directly, while DOD still serves as the point of contact for participating DIB contractors.

Authorities

Authorities for U.S. military operations in cyberspace are not currently organized according to the nature of the perceived threat, whether espionage, crime, or war. Instead, authorities are organized according to the domain (.mil, .gov, .com, etc.) in which the activity is taking place, as opposed to its motivations or effects. Presidential Policy Directive 20, discussed in greater detail below, distinguishes between *network defense* on the one hand and *offensive and defensive cyberspace operations* on the other.

U.S. policy on network defense is to adopt a risk-management framework published by the Department of Commerce's National Institute of Standards and Technology. Responsibility for implementing the framework is shared among different government departments and agencies, with U.S. Cyber Command responsible for the .mil domain and the Department of Homeland Security responsible for the .gov domain. Adoption of the NIST framework is voluntary for private companies and their own network defense.

One of the instruments through which offensive cyberspace operations are conducted may be a classified "Execute Order," defined by DOD as an order issued by the Chairman of the Joint Chiefs of Staff, at the direction of the Secretary of Defense, to implement a decision by the President to initiate military operations.[57] According to The Federation of American Scientists' *Secrecy News,* Air Force Instruction 10-1701, entitled "Command and Control (C2) for Cyberspace Operations," dated March 5, 2014, states, "Classified processes governing C2 [command and control] of AF [Air Force] offensive and defensive cyberspace operations conducted by AF Cyber Mission Forces are addressed in a classified CJCS [Chairman, Joint Chiefs of Staff] Execute Order (title classified) issued on 21 Jun 13."[58] Then-Vice Admiral Michael Rogers, as a nominee for Commander, U.S. Cyber Command (and NSA Director), said before the Senate Armed Services Committee that "geographic combatant commanders already have authority to direct and execute certain Defensive Cyberspace Operations (DCO) within their own networks." However, the Execute Order suggests that there may be standing orders to conduct offensive cyberspace operations as well.

The following section provides a brief overview of evolving norms in cyberspace and the authorities that govern network defense and cyberspace operations.

Legislative Authorities

Section 941of [*sic*] the National Defense Authorization Act for Fiscal Year 2013 (P.L. 112-239), affirms the Secretary of Defense's authority to conduct military activities in

[57] DOD Dictionary of Military and Associated Terms, JP1-02.

[58] U.S. Military Given Secret "Execute Order" on Cyber Operations Military Doctrine, Secrecy http://blogs.fas.org/secrecy/2014/03/execute-order/.

cyberspace. The provision's language is similar to that in Section 954 of final conference report to accompany H.R. 1540, the National Defense Authorization Act for Fiscal Year 2012. In this version, this section reaffirms that the Secretary of Defense has the authority to conduct military activities in cyberspace. In particular, it clarifies that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to a congressionally authorized use of force outside of the United States, or to defend against a cyberattack on an asset of the DOD.[59] The section highlights the blurred lines between military operations and intelligence activities, particularly with respect to cyberspace. In general, Title 10 and Title 50 of the U.S. Code refer to distinct chains of command and missions belonging to the armed forces and intelligence agencies, respectively. The U.S. Cyber Command, the military entity responsible for offensive operations in cyberspace and subject to Title 10 authorities, is co-located with and led by the Director of the National Security Agency, a Title 50 intelligence organization. Computer Network Attack, the military parlance for offensive operations, is closely related to and at times indistinguishable from Computer Network Exploitation, which is used to denote data extrapolation or manipulation.

According to DOD, a clandestine operation is one that is "sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of the identity of the sponsor."[60] Under Title 50, a "covert action" is subject to presidential finding and Intelligence Committee notification requirements. Traditional military activity, although undefined, is an explicit exception to the Title 50 U.S.C. covert action definition in Section 913 as the identity of the sponsor of a traditional military activity may be well known.

According to the Joint Explanatory Statement of the Committee of Conference, H.R. 1455, July 25, 1991, traditional military activities

> include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.

By this reading, a clandestine operation falls under the traditional military activity rubric, because the identity of the sponsor is not concealed. Hence, by referring only to "clandestine" operations rather than covert operations, the provision distinguishes between approval and reporting requirements for military-directed cyberspace operations and those conducted by the intelligence community. By requiring quarterly

[59] The previous version would have given the Secretary of Defense the authority to conduct clandestine cyberspace activities in support of military operations pursuant specifically to the Authorization for the Use of Military Force (P.L. 107-40; 50 U.S.C. 1541 note) outside of the United States or to defend against a cyberattack on an asset of the Department of Defense.

[60] Department of Defense Dictionary of Military and Associated Terms, Joint Publication1-02, as amended through August 15, 2014. [reconcile with similar footnote above] [*sic*]

briefings to the congressional defense committees, the language would also appear to address concerns that a "clandestine" or "traditional military activity" designation for a cyber operation would skirt the strict oversight requirements of its covert counterpart. However, confusion may remain regarding the proper role and requirements of the military, because some cyber operations may contain both covert and clandestine elements. Another consideration is the military's responsibility to notify congressional intelligence committees of computer network exploitation activities undertaken as "operational preparation of the environment."

Executive Authorities

In December 2008, President-elect Obama offered details about the cybersecurity goals his Administration would pursue, including "strengthening federal leadership on cybersecurity, developing next-generation secure computers and networking for national security applications, and protecting the IT infrastructure to prevent corporate cyberespionage."[61] In February 2009, he initiated a 60-day interagency review with the goal of developing "a strategic framework to ensure" that federal cybersecurity initiatives "are appropriately integrated, resourced, and coordinated with Congress and the private sector."[62] The White House released the *Cyberspace Policy Review* in May 2009.[63] At that time, the President announced[64] that the Administration would "pursue a new comprehensive approach to securing America's digital infrastructure," and that he was creating a new White House office to be led by a Cybersecurity Coordinator—a senior cybersecurity policy official, often referred to as the "Cyber Czar," assigned to the Office of the President and responsible for coordinating the nation's cybersecurity-related policies.

While many security observers saw these initial efforts by the Obama Administration as a positive step, others were concerned that government-wide collaborative efforts were not keeping pace with the threats directed at U.S. technological global interests. Between 2009 and 2013, cyber threats to U.S. infrastructure and other assets became a growing concern to policy makers.[65]

In the absence of legislative action, in 2012 the Obama Administration announced a new Presidential policy directive related to U.S. Cyber Operations, the contents of which remain classified, and began drafting an executive order on cybersecurity practices,

[61] "Report: White House should oversee cybersecurity," *CNN*, December 8, 2008, http://www.cnn.com/2008/TECH/12/08/cyber.security/.

[62] The White House, "President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review," press release, February 9, 2009, http://www.whitehouse.gov/the-press-office/president-obama-directs-national-security-and-homeland-security-advisors-conduct-im.

[63] The White House, *Cyberspace Policy Review*, May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; the White House, "Cyberspace Policy Review [Supporting Documents]," May 2009, http://www.whitehouse.gov/cyberreview/documents/.

[64] The White House, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," press release, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[65] CRS Report R41674, *Terrorist Use of the Internet: Information Operations in Cyberspace*, by Catherine A. Theohary and John W. Rollins; CRS Report R42507, *Cybersecurity: Authoritative Reports and Resources, by Topic*, by Rita Tehan.

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, released after a year of interagency debate and review.

At the federal level, five executive orders and Presidential directives authorize offensive and defensive action in cyberspace:

National Security Presidential Directive 54/Homeland Security Presidential Directive 23—The Comprehensive National Cybersecurity Initiative

The Obama Administration's *Cyberspace Policy Review* builds on the Comprehensive National Cybersecurity Initiative (CNCI) launched in January 2008 by the George W. Bush Administration via a classified presidential directive.[66] The CNCI established a multipronged approach for the federal government to identify threats, address telecommunications and information-system vulnerabilities, and respond to or proactively address entities that wish to steal or manipulate protected data on secure federal systems.[67]

Presidential Policy Directive 20 (PPD-20)—U.S. Cyber Operations Policy

President Obama implemented PPD-20 on U.S. Cyber Operations Policy in October 2012. Although subsequently leaked to the public in June of 2013,[68] PPD-20's contents remain classified, with the exception of what the White House shared in a brief fact sheet. A widely cited *Washington Post* article published on November 14, 2012 asserted the significance of PPD-20:

> For the first time…the directive explicitly makes a distinction between network defense and cyber-operations to guide officials charged with making often-rapid decisions when confronted with threats. The policy also lays out a process to vet any operations outside government and defense networks and ensure that U.S. citizens' and foreign allies' data and privacy are protected and international laws of war are followed.

The article went on to quote an unnamed senior administration official on the distinction between defense and offense, clarifying that "network defense is what you're doing inside your own networks.… Cyber-operations is stuff outside that space, and recognizing that you could be doing that for what might be called defensive purposes."[69]

PPD-20 closes a perceived gap in the authorities necessary for DOD to defend the nation in cyberspace, a gap that has not been addressed by Congress. The directive does not create new powers for federal agencies or the military; however, by distinguishing between network defense and cyber operations, it provides a policy framework for the

[66] "The Comprehensive National Cybersecurity Initiative," http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative; National Security Presidential Directive 54 /Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

[67] CRS Report R40427, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John W. Rollins and Anna C. Henning.

[68] Joshua Eaton, "American cyber-attack list uncovered," *Al Jazeera*, http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html, accessed August 12, 2014.

[69] Ellen Nakashima, "Obama Signs Secret Directive to Help Thwart Cyberattacks" *Washington Post*, November 14, 2012.

Pentagon's rules of engagement for cyberspace. As specifically described in the White House fact sheet, PPD-20:

- takes into account the evolution of the threat and growing experience with the threat;
- establishes principles and processes for using cyber operations so cyber tools are integrated with the full array of national security tools;
- provides a whole-of-government approach consistent with values promoted domestically and internationally and articulated in the International Strategy for Cyberspace;
- mandates that the United States take the least action necessary to mitigate threats; and
- prioritizes network defense and law enforcement as preferred courses of action.[70]

Executive Order 13636—Improving Critical Infrastructure Cybersecurity

The White House released EO 13636 on February 12, 2013. This executive order declares that "it is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure (CI) and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (Section 1). The order:

- expands information sharing and collaboration between the government and the private sector, including sharing classified information by broadening a program developed for the defense industrial base to other CI sectors;
- develops a voluntary framework of cybersecurity standards and best practices for CI protection, through a public/private effort;
- establishes a consultative process for improving CI cybersecurity;
- identifies CI with especially high priority for protection, using the consultative process;
- establishes a program with incentives for voluntary adoption of the framework by CI owners and operators;
- reviews cybersecurity regulatory requirements to determine whether they are sufficient and appropriate; and
- incorporates privacy and civil liberties protections in activities under the order.

In addition to codifying the DECS program, the order provides specific responsibilities to DHS and the sector-specific agencies, as well as the Departments of Commerce, Defense, and Justice, the intelligence community, the General Services Administration, and the Office of Management and Budget, addressed below.

[70] Cheryl Pellerin, "DOD Readiness Elements Crucial to Cyber Operations" U.S. Department of Defense, American Forces Press Service, http://www.defense.gov/news/newsarticle.aspx?id=120381.

Presidential Policy Directive 21—Critical Infrastructure Security and Resilience

Along with EO 13636, the White House released Presidential Policy Directive 21 (PPD-21),[71] "Critical Infrastructure Security and Resilience," which addresses the protection of CI. PPD-21 supersedes Homeland Security Presidential Directive 7 (HSPD 7), "Critical Infrastructure Identification, Prioritization, and Protection," released December 17, 2003. PPD-21 seeks to strengthen the security and resilience of CI by

- clarifying functional relationships among federal agencies, including the establishment of separate DHS operational centers for physical and cyber-infrastructure;
- identifying baseline requirements for information sharing;
- applying integration and analysis capabilities in DHS to prioritize and manage risks and impacts, recommend preventive and responsive actions, and support incident management and restoration efforts for CI; and
- organizing research and development (R&D) to enable secure and resilient CI, enhance impact-modeling capabilities, and support strategic DHS guidance.

The directive provides specific responsibilities to DHS and the sector-specific agencies, as well as the Departments of Commerce, Interior, Justice, and State; the intelligence community; the General Services Administration; and the Federal Communications Commission.

National Infrastructure Protection Plan, National Response Framework and Defense Support for Civil Authorities

The National Infrastructure Response Plan (NIPP), developed by DHS with other federal agencies and private sector owners of critical infrastructure, outlines how government and private sector critical infrastructure stakeholders work together to manage risks and achieve security and resiliency. The NIPP 2013 meets the requirements of PPD-21, "Critical Infrastructure and Resilience."

The phrase "defense support of civil authorities" refers to DOD's mission to help civil authorities respond to a domestic emergency or other domestic activity. This support may be provided through the military services, the National Guard, and other DOD resources. For the civil cybersecurity mission, DHS leads the interagency with DOD support. The National Cyber Incident Response Plan outlines roles and responsibilities for coordinating and executing a response to a domestic cyber incident.[72] This plan fits into DHS's National Response Framework, a tiered response guide for local, state, and federal governments with respect to major disasters or emergencies. A 2010 memorandum of agreement between DOD and DHS also guides cooperation between the two entities with respect to securing national cyber assets.[73]

---

[71] The White House, "Critical Infrastructure Security and Resilience," *Presidential Policy Directive 21*, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[72] Department of Homeland Security, National Cyber Incident Response Plan, Interim Version, September 2010.

[73] Accessed at https://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

International Authorities

The DOD's role in defense of cyberspace follows the body of laws, strategies, and directives outlined above. For the military to respond to an act of cyberterrorism or cyberwar, a presidential finding must be issued and an order must be executed. However, discussions have been underway in various international fora that may affect how the U.S. government views certain actions in cyberspace and when a military response is warranted. Although the President still decides ultimately what the military will do, the decisions made in the international arena could affect how the Department of Defense organizes, trains, and equips its forces in order to fulfill treaty obligations.

As of yet, no international instruments have been drafted explicitly to regulate interstate relations in cyberspace. One apparent reason for the absence of such a treaty is that the international governance of cyberspace has largely been the purview of private, professional organizations such as the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN). However, politically motivated cyberattacks are increasingly common and, although difficult to attribute, often raise strong suspicion of government involvement. More importantly, perhaps, states have become targets of cyberattack, provoking a sense of urgency regarding the creation of national strategies and capabilities for cyberdefense and cyberoffense.

The U.S. Position on International Authorities

The Obama Administration has responded to the internationalization of the cyberspace threat environment by releasing in 2011 an *International Strategy for Cyberspace*.[74] The Strategy calls for strengthening bilateral and multilateral government partnerships, and a strong role for the private sector. It does not call for any new treaties or agreements, and the only existing instrument cited is the Budapest Convention (discussed below). It recommends, instead, preservation of the openness that has been a hallmark of the Internet age. This puts the United States at odds with China and Russia, both of which prefer a more nationalistic approach to Internet governance.

In September 2012, the U.S. State Department, for the first time, took a public position on whether cyber activities could constitute a use of force under Article 2(4) of the U.N. Charter and customary international law. According to State's then-legal advisor, Harold Koh, "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[75] Examples offered in Koh's remarks included triggering a meltdown at a nuclear plant, opening a dam and causing flood damage, and causing airplanes to crash by interfering with air traffic control. By focusing on the ends achieved rather than the means with which they are carried out, this definition of cyberwar fits easily within existing international legal frameworks. If an actor employs a cyber weapon to produce kinetic effects that might warrant fire power under other circumstances, then the use of that cyber weapon rises to the level of the use of force.

[74] The White House, *International Strategy for Cyberspace*, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[75] Remarks of Harold Hongju Koh, Legal Advisor U.S. Department of State, at a USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012.

However, the United States recognizes that cyberattacks without kinetic effects are also an element of armed conflict under certain circumstances. Koh explained that cyberattacks on information networks in the course of an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyberattack with a proportional use of kinetic force. In addition, "computer network activities that amount to an armed attack or imminent threat thereof" may trigger a nation's right to self-defense under Article 51 of the U.N. Charter. Here Koh cites the *International Strategy for Cyberspace*, which affirmed that "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." The International Strategy goes on to say that the U.S. reserves the right to use all means necessary—diplomatic, informational, military, and economic—as appropriate and consistent with applicable law, and exhausting all options before military force whenever possible.

International Consensus-Building Activities

One of the Defense Objectives of the *International Strategy for Cyberspace* is to work internationally "to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend national assets." A growing awareness of the threat environment in cyberspace has led to two major international processes geared toward developing international expert consensus international cyber authorities.

First, the threat environment has spurred NATO interest in understanding how existing international law applies to cyberwarfare. A year after the 2007 DDoS attack on Estonia, NATO established the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, Estonia. The CCDCOE hosts workshops and courses on law and ethics in cyberspace, as well as cyber-defense exercises. In 2009, the center convened an international group of independent experts to draft a manual on the law governing cyberwarfare. The Tallinn Manual, as it is known, was published in 2013. It sets out 95 "black letter rules" governing cyber conflict addressing sovereignty, state responsibility, the law of armed conflict, humanitarian law, and the law of neutrality. The Tallinn Manual is an academic text: although it offers reasonable justifications for the application of international law, it is non-binding and the authors stress that they do not speak for NATO or the CCDCOE.

Second, the cyberspace threat environment has prompted the United Nations to convene Groups of Governmental Experts (GGE) to study "Developments in the Field of Information and Telecommunications in the Context of International Security." The first successful U.N. GGE report came out in 2010, followed by a second report in 2013. The current GGE is expected to reach consensus again in 2015. The stated purpose of this process is to build "cooperation for a peaceful, secure, resilient and open ICT environment" by agreeing upon "norms, rules and principles of responsible behaviour by States" and identifying confidence and capacity-building measures, including for the exchange of information. Unlike the work done at Tallinn under the auspices of NATO, this U.S.-led process includes both China and Russia.

Existing International Instruments That Bear on Cyberwarfare

As previously discussed, the military's role in cyberwarfare is governed by U.S. law. Yet many international instruments bear on cyberwarfare, including those relating to law enforcement (e.g., extradition and mutual legal assistance treaties), defense, and security, along with broad treaties and agreements, such as the United Nations Charter and the Geneva Conventions, as well as international law. Such instruments include, but are not limited to, those described below.

Council of Europe Convention on Cybercrime

This law-enforcement treaty, also known as the Budapest Convention, requires signatories to adopt criminal laws against specified types of activities in cyberspace, to empower law-enforcement agencies to investigate such activities, and to cooperate with other signatories. Those activities include both attacks on the integrity of cyber-systems and content-related crimes such as fraud, pornography, and "hate speech." The convention focuses on identification and punishment of criminals rather than prevention of cybercrime. Consequently, it may act as a deterrent, but it has no remediating effect on the criminal acts that do occur. Also, the provisions on content may not be consistent with the different approaches of various nations to freedom of expression. While widely cited as the most substantive international agreement relating to cybersecurity, some observers regard it as unsuccessful.[76]

In addition to most members of the Council of Europe, the United States and three other nations have ratified the treaty.[77]

United Nations Resolutions

A series of U.N. General Assembly resolutions relating to cybersecurity have been adopted over the past 15 years. One resolution called for a report from an international group of government experts from 15 nations, including the United States. That 2010 report, sometimes referred to as the Group of Governmental Experts (GGE) Report, recommended a series of steps to "reduce the risk of misperception resulting from ICT[78] disruptions" but did not incorporate any binding agreements.[79] Nevertheless, some observers believe the report represents progress in overcoming differences between the

[76] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View" Future Challenges Essay, June 2, 2011, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf. He cites "vague definitions," reservations by signatories, and loopholes as reasons for its lack of success.

[77] Council of Europe, "Convention on Cybercrime, CETS No. 185," accessed February 18, 2013, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG. See also Michael Vatis, "The Council of Europe Convention on Cybercrime," in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (Washington, DC: National Academies Press, 2010), pp. 207–223.

[78] The abbreviation ICT, which stands for information and communications technologies, is increasingly used instead of IT, (information technologies) because of the convergence of telecommunications and computer technology.

[79] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, July 30, 2010, http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201.

United States and Russia about various aspects of cybersecurity.[80] In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society (WSIS) to discuss on information society opportunities and challenges. This summit was first convened in Geneva, in 2003, and then in Tunis, in 2005, and a10-year follow-on in Geneva in May 2013. Delegates from 175 countries took part in the first summit, where they adopted a Declaration of Principles—a road map for achieving an open information society. The Geneva summit left other, more controversial issues unresolved, including the question of Internet governance and funding. At both summits, proposals for the United States to relinquish control of ICANN were rejected.

Law of War

The so-called "Law of War" embodied in the Geneva and Hague Conventions and the U.N. Charter may in some circumstances apply to cyberattacks, but without attempts by nation states to apply it, or specific agreement on its applicability, its relevance remains unclear. It is also complicated by difficulties in attribution, the potential use of botnets (see the "Malware" section above), and possible harm to third parties from cyber-counterattacks, which may be difficult to contain. In addition, questions of territorial boundaries and what constitutes an armed attack in cyberspace remain. The law's application would appear clearest in situations where a cyberattack causes physical damage, such as disruption of an electric grid. As mentioned above, the Tallinn Manual addresses many of these questions.[81]

International Law on Countermeasures

This body of international law relates to "how states may respond to international law violations that do not rise to the level of an armed attack justifying self-defense." It does not expressly address cyberattacks but presumably would be applicable to them, provided the countermeasures target the responsible nation and are "temporary and instrumentally directed" to induce cessation of the violation.[82] Similar caveats apply to such countermeasures with respect to attribution and effects on innocent parties.

North Atlantic Treaty Organization (NATO)

Since the 2007 attack on Estonia,[83] NATO has established authorities relating to cyberdefense, with the goals of advancing strategy and centralizing defense capabilities across

[80] Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review 100*, no. 4 (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.

[81] For a detailed discussion, see Hathaway et al., "The Law of Cyber-Attack." See also CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary; James A. Lewis, Conflict and Negotiation in Cyberspace (Center for Strategic and International Studies, February 2013), https://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf; Mary Ellen O'Connell and Louise Arimatsu, Cyber Security and International Law (London, UK: Chatham House, May 29, 2012), http://www.tsa.gov/sites/default/files/assets/pdf/Intermodal/pipeline_sec_incident_recvr_protocol_plan.pdf.

[82] Hathaway et al., "The Law of Cyber-Attack," p. 857.

[83] See CRS Report RL31787, *Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues*, by Catherine A. Theohary.

members. A policy on cyberdefense[84] and an associated action plan were adopted in 2011, and the NATO Communications and Information Agency (NCIA) was established in 2012 to facilitate the centralization effort.[85] The NATO Cyber Center of Excellence located in Tallinn, Estonia, is another source of legal analysis.

International Telecommunications Regulations

The International Telecommunication Union (ITU) regulates international telecommunications through binding treaties and regulations and nonbinding standards. Regulations prohibit interference with other nations' communication services and permit control of non-state telecommunications for security purposes. The regulations do not, however, expressly forbid military cyberattacks. Also, ITU apparently has little enforcement authority.[86]

Other International Law

Some bodies of international law, especially those relating to aviation and the sea, may be applicable to cybersecurity; for example by prohibiting the disruption of air traffic control or other conduct that might jeopardize aviation safety.[87] Bilaterally, mutual legal assistance treaties between countries may be applicable for cybersecurity forensic investigations and prosecution.

Defense Instruments

The United States has signed 16 treaties and other agreements with 13 other countries and the European Union that include information security, mostly of classified military information, or defense-related information assurance and protection of computer networks. According to news reports, the United States and Australia have agreed to include cybersecurity cooperation within a defense treaty, declaring that a cyberattack on one country would result in retaliation by both.[88]

Other International Organizations

A number of regional associations of nation states have issued declarations of goals and statements of intent relating to cybersecurity, including:

- the G8 Group of States,

[84] The concept document (available at http://www.nato.int/cps/en/natolive/official_texts_68580.htm) states that NATO will "develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyberdefence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations."

[85] North Atlantic Treaty Organization, "NATO and Cyber Defence," February 19, 2013, http://www.nato.int/cps/en/SID-537741AA-89F4BEF4/natolive/topics_78170.htm?.

[86] Hathaway et al., "The Law of Cyber-Attack." See also Anthony Rutkowski, "Public International Law of the International Telecommunication Instruments: Cyber Security Treaty Provisions Since 1850," Info 13, no. 1 (2011): 13–31, http://www.emeraldinsight.com/journals.htm?issn=1463-6697&volume=13&issue=1&articleid=1893240& show=pdf&PHPSESSID=9r0c5maa4spkkd9li78ugbjee3.

[87] Hathaway et al., "The Law of Cyber-Attack."

[88] See, for example, Lolita Baldor, "Cyber Security Added to US-Australia Treaty," Security on NBCNews.com, 2011, http://www.msnbc.msn.com/id/44527648/ns/technology_and_science-security/t/cyber-security-added-us-australia-treaty/.

- the Asian Pacific Economic Cooperation (APEC),
- the Organization of American States (OAS),
- the Association of South East Asian Nations (ASEAN),
- the Arab League, and
- the Organization for Economic Cooperation and Development (OECD).

However, none of the documents issued by these organizations appear to be binding in effect.[89]

SCO-Proposed International Code of Conduct for Information Security

In September 2011, members of the Shanghai Cooperation Organization, including Russia and China, submitted a proposed voluntary code of conduct for cybersecurity and requested that it be placed on the U.N. General Assembly agenda.[90] Its focus on the rights of governments, such as "reaffirming that policy authority for Internet-related public issues is the sovereign right of States," among other concerns, led to resistance from the United States and other countries.[91]

OSCE Early Warning Resolution

Under the auspices of the Organization for Security and Cooperation in Europe (OSCE), in 2011 and 2012, the United States, Russia, and other countries negotiated a possible agreement that would warn parties early on when cyber-operations might lead to unintentional conflict, but they were unable to reach consensus on the resolution.[92] Although some observers have expressed interest in such an agreement, others doubt its effectiveness, arguing that conflicting interests and the difficulties of attribution, among other problems, make it unfeasible.[93]

ITU Dubai Summit

The ITU convened the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates, during December 3–14, 2012, to review the International Telecommunications Regulations. In the run-up to the summit, many security observers

[89] For summaries, see International Telecommunication Union, Global Cybersecurity Agenda (GCA): *Global Strategic Report*, 2008, http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf.

[90] Ministry of Foreign Affairs of the People's Republic of China, "China, Russia and Other Countries Submit the Document of International Code of Conduct for Information Security to the United Nations," September 13, 2011, http://www.fmprc.gov.cn/eng/zxxx/t858978.htm.

[91] Among the concerns cited were the absence of provisions on international law enforcement and combating cyberespionage; its call for international cooperation relating to "curbing dissemination of information" relating to "political, economic, and social stability" and "spiritual and cultural environment"; and ambiguity with respect to censorship policy (Jeffrey Carr, "4 Problems with China and Russia's International Code of Conduct for Information Security," *Digital Dao*, September 22, 2011, http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html).

[92] Aliya Sternstein, "U.S., Russia, Other Nations Near Agreement on Cyber Early-Warning Pact," *Nextgov: Cybersecurity*, December 5, 2012, http://www.nextgov.com/cybersecurity/2012/12/us-russia-other-nations-near-agreement-cyber-early-warning-pact/59977/; Aliya Sternstein, "Cyber Early Warning Deal Collapses After Russia Balks," *Nextgov: Cybersecurity*, December 7, 2012, http://www.nextgov.com/cybersecurity/2012/12/cyber-early-warning-deal-collapses-after-russia-balks/60035/.

[93] Goldsmith, "Cybersecurity Treaties: A Skeptical View."

expressed concern over the closed nature of the talks and feared a shift of Internet control away from private entities such as ICANN toward the U.N. and national governments. Although these concerns proved to be largely baseless, a controversial deep packet inspection proposal from the People's Republic of China was adopted at the summit.[94] Dissenting countries, including Germany, fear that this recommendation will result in accelerated Internet censorship in repressed nations.

Issues for Congress

Authorities: Is Current Law Enough?

Does the military have the authorities it needs to effectively fight and win wars in cyberspace? Some have argued that to fulfill its homeland defense mission, USCYBERCOM should be given increased authority over private sector critical infrastructure protection. Yet business owners, particularly in the IT sector, contend that this would represent a "militarization of cyberspace" that would create distrust among consumers and shareholders, and could potentially stifle innovation, leading to decreases in profits. Others argue that the military's role is to fight and win wars, rather than to bolster a private company's cyber defenses.

As discussed, the international community must contend with a certain amount of ambiguity regarding what constitutes an "armed attack" attack in cyberspace and what the thresholds are for cyberattack as an act of war, an incident of national significance, or both. Without clear redlines and specific consequences articulated, deterrence strategies may be incomplete. On the other hand, a lack of redlines and consequences could constitute a form of strategic ambiguity that gives the U.S. military operational maneuverability. Congress may wish to consider these concerns as new legislation regarding critical infrastructure protection is proposed.

Skilled cyber operators are in demand in the military, and the national supply of cyber professionals tends to reside in the private sector. Some of the services are looking at bolstering opportunities for officers who wish to pursue careers in cybersecurity by creating new occupational specialties and career tracks. Yet barriers to hiring skilled civilians for the DOD cyber mission may hinder the development of a robust workforce. Congress may choose to consider ways to incentivize and bolster recruitment of talent outside of the military, such as providing special hiring authorities for certain mission critical positions, streamlining or revising the clearance process for national security personnel, and compensation comparable to private sector equivalent jobs.

How Do DOD and Cyber Command Responsibilities for Cybersecurity Fit Within the Interagency and Private Sector?

Reports have described the USCYBERCOM cyber force's "National Mission Teams" as protecting the networks that undergird critical infrastructure. Given that the majority of this critical infrastructure resides in the private sector, for which DHS has coordinating authority, how do USCYBERCOM teams protect these assets during peacetime without violating *Posse Comitatus*, the prohibition against using the military for domestic policing? How do these national teams interact and coordinate with DHS?

[94] Deep packet inspection allows the content of a unit of data to be examined as it travels through an inspection point, a process which enables data mining and eavesdropping programs.

Should U.S. Cyber Command Be Its Own Unified Combatant Command?

The Unified Command Plan organizes combatant commands into geographic and functional areas. U.S. Cyber Command is currently organized under the functional Strategic Command, and co-directed and located with the National Security Agency (NSA). With the complicated lines of authority (Title 10 vs. Title 50) associated with this structure, some have suggested separating the two organizations and giving civilian control to the NSA while elevating Cyber Command to the level of a full unified combatant command. DOD has been tasked by Congress to study and report on the possible implications of this realignment. Specifically, The National Defense Authorization Act for Fiscal Year 2013 (P.L. 112-239) asks in Section 940 "how a single individual could serve as a commander of a combatant command that conducts overt, though clandestine, cyber operations under Title 10, United States Code, and serve as the head of an element of the intelligence community that conducts covert cyber operations under the National Security Act of 1947."

Is a Separate Cyber Force Necessary?

Given that the DOD views cyberspace as one of five global domains, some proponents in Congress contend that a separate cyber force, akin to the Army, Navy, Air Force, or Marine Corps, is necessary to properly address the military aspects of the domain. However, critics point to the multi-layered aspect of cyberspace in which all services have equities.

What Are the Authorizing and Oversight Committees and Jurisdictional Implications?

As previously discussed, blurred lines between operations undertaken under Title 10 and Title 50 authorities can complicate efforts to determine the chain of command and jurisdictional review process. What does this ambiguity mean for congressional oversight committees? Have some operations taken place without congressional notification? What has been the Department of Defense's role in responding to cyberattacks on private networks?

Current Legislation

The National Defense Authorization Act for Fiscal Year 2015 (P.L. 113-291) contains some provisions related to DOD cybersecurity and cyber operations. These provisions:

- require reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors.
- require the Principal Cyber Advisor to identify improvements to ensure sufficient civilian workforce to support USCYBERCOM and components.
- direct a program of decryption to inspect content for threats and insider activity within DOD networks.
- state the Sense of Congress that as ICANN turns to global community for leadership, support should be given only if assurances are provided for current legacy IP numbers used by DOD and the U.S. government.

- direct that a new mission forces, training, manning and equipping plan and associated programmatic elements be submitted to Congress.
- state a Sense of Congress for consideration regarding role of reserve components in defense against cyberattacks given their unique experience in private and public sectors and existing relationships with local and civil authorities for emergency response.

Appendix. Timeline of International Attacks[95]

February–June 1999: Kosovo was the arena for the first large-scale Internet war, involving pro-Serbian forces cyberattacking the North Atlantic Treaty Organization (NATO). As NATO planes bombed Serbia, pro-Serbian hacker groups, such as the "Black Hand," attacked NATO, U.S., and UK Internet infrastructure and computers via DoS attacks and virus-infected email. In the United States, the White House website was defaced. The UK admitted to losing database information. At NATO Headquarters in Belgium, a public affairs website for the war in Kosovo was "virtually inoperable for several days." Simultaneously, NATO's email server was flooded and choked with email.[96] During the Kosovo conflict, a NATO jet bombed the Chinese embassy in Belgrade in May 1999. The Chinese Red Hacker Alliance retaliated by launching thousands of cyberattacks against U.S. government websites.[97]

October 2000: Riots in the Palestinian territories sparked rounds of cyberattacks between Israelis and Palestinians. Pro-Israeli attacks targeted the official websites of the Palestinian Authority, Hamas, and the government of Iran. Pro-Palestinian hackers retaliated against Israeli political, military, telecommunications, media, the financial sector, commercial, and university websites. Since 2000, the Middle East cyberwar has kept pace with the ground conflict.[98]

April–May 2007: DDoS attacks shutdown websites of Estonia's parliament, banks, ministries, newspapers, and broadcasters. Estonian officials accused the Russian government of responding to their decision to move a Soviet-era war memorial with retaliatory cyberattacks.[99]

September 2007: Israel disrupted Syrian air defense networks during the bombing of an alleged nuclear facility in Syria.[100]

---

[95] Unless otherwise noted, these events are cited in "Significant Cyber Events" Washington, DC: Center for Strategic and International Studies, http://csis.org/program/significant-cyber-events; accessed August 7, 2014.

[96] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," keynote speech, Japan, 2008, http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

[97] Jeffrey Carr, "Real Cyber Warfare: Carr's Top Five Picks," *Forbes*, February 4, 2011, http://www.forbes.com/sites/jeffreycarr/2011/02/04/real-cyber-warfare-carrs-top-five-picks/; Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," keynote speech, Japan, 2008, http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

[98] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," keynote speech, Japan, 2008, http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf.

[99] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

[100] "Significant Cyber Events" Washington, DC: Center for Strategic and International Studies, http://csis.org/program/significant-cyber-events; accessed August 7, 2014.

July 2008: Government and corporate websites in Lithuania were defaced. The Soviet-themed graffiti implicated Russian nationalist hackers.[101]

August 2008: Georgian government and commercial websites were shut down by DoS attacks at the same time that Russian ground troops invaded the country.[102]

January 2009: DoS attacks originating in Russia shut down Kyrgyzstan's two main Internet servers on the same day that the Russian government pressured Kyrgyzstan to bar U.S. access to a local airbase.[103]

July 2009: Servers in South Korea and the United States sustained a series of attacks, reportedly by North Korea.[104]

June 2010: "Stuxnet" worm damaged an Iranian nuclear facility. The United States and Israel were implicated in the attack.[105]

September 2011: "Keylogger" malware was found on ground control stations for U.S. Air Force unmanned aerial vehicles (UAVs) and reportedly infected both classified and unclassified networks at Creech Air Force Base in Nevada.

May 2012: An espionage worm called "Flame," allegedly 20 times more complex than Stuxnet, was discovered on computers in the Iranian Oil Ministry, as well as in Israel, Syria, and Sudan.

August 2012: "Gauss" worm infected 2,500 systems worldwide. The malware appeared to have been aimed at Lebanese banks, and contained code whose encryption has not yet been broken.

August 2012: The "Cutting Sword of Justice," a group reportedly linked to the government of Iran, used the "Shamoon" virus to attack major oil companies including Aramco, a major Saudi oil supplier, and the Qatari company RasGas, a major liquefied natural gass (LNG) supplier. The attack on Aramco deleted data on 30,000 computers and infected (without causing damage) control systems.

September 2012–June 2013: The hacker group Izz ad-Din al-Qassam launched DoS attacks against major U.S. financial institutions in "Operation Ababil." Izz ad-Din al-Qassam is believed to have links to Iran and Hamas.

January 2013: The *New York Times*, *Wall Street Journal*, *Washington Post*, and *Bloomberg News* revealed that they were targeted by persistent cyberattacks. China was the suspected source.

---

[101] Brian Krebs, "Lithuania Weathers Cyberattack, Braces for Round 2," *The Washington Post*, July 3, 2008, http://voices.washingtonpost.com/securityfix/2008/07/lithuania_weathers_cyber_attac_1.html.

[102] John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

[103] Daniel McLaughlin, "Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites" (*Irish Times*, July 2, 2008) p. 10, http://lumen.cgsccarl.com/login?url=http://proquest.umi.com/pqdweb? did=1503762091&sid=2&Fmt=3&clientld=5094&RQT=309&VName=PQD.

[104] "Significant Cyber Events" Washington, DC: Center for Strategic and International Studies, http://csis.org/program/significant-cyber-events; accessed August 7, 2014.

[105] Ralph Langer, "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve," November, 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

May 2013: Israeli officials reported a failed attempt by the Syrian Electronic Army to compromise water supply to the city of Haifa.

August 2013: Leaks revealed that the U.S. government purportedly conducted 231 cyber intrusions in 2011 against Russia, China, North Korea, and Iran. Most of the intrusions were related to nuclear proliferation.

April 2014: The disclosure of the Heartbleed bug revealed vulnerability in the OpenSSL protocol previously considered the standard for Internet security. Canada reported more than 900 compromised social security numbers.[106]

May 2014: The United States indicted five Chinese military officers on charges of computer hacking, economic espionage, and other offenses against six targets in the United States' nuclear power, metals, and solar power industries. China has denied the charges.[107] According to U.S. Attorney General Eric Holder, "This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking."[108]

July 2014: The United States charged a Chinese entrepreneur with breaking into the computer systems of the U.S. defense giant Boeing and other firms to steal data on military programs concerning warplanes, including C-17 cargo aircraft, and the F-22 and F-35 fighter jets.[109] At the same time, the security firm Kapersky reported a massive cyber operation dubbed "Energetic Bear," which targeted more than 2,800 industrial firms around the globe. Although some reports identified a Russian hacker group as the source, Kapersky refrained from attributing the attack to any one country.[110]

December 2014: U.S. cybersecurity firm Cylance reported that an Iranian hacker group has breached airlines, energy and defense firms, and the U.S. Marine Corps intranet in an attack known as "Operation Cleaver."[111]

Author Contact Information

Catherine A. Theohary
Specialist in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844

Anne I. Harrington
APSA Congressional Fellow

[106] http://heartbleed.com; "OpenSSL Heartbleed Vulnerability" Cyber Security Bulletins. Public Safety Canada. April 11, 2014, retrieved April 14, 2014. SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser.

[107] Song Sang-ho, "Concerns rise over militarization of cyberspace," *The Korean Herald*, July 13, 2014, http://www.koreaherald.com/view.php?ud=20140713000188.

[108] Office of Public Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, Department of Justice, May 19, 2014, http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

[109] Dan Levine, "US Charges Chinese Man with Hacking into Boeing," *Reuters*, July 11, 2014, http://www.reuters.com/article/2014/07/11/boeing-china-cybercrime-idUSL2N0PM2FV20140711.; Song Sang-ho, "Concerns rise over militarization of cyberspace," *The Korean Herald*, July 13, 2014, http://www.koreaherald.com/view.php?ud=20140713000188.

[110] See http://www.darkreading.com/attacks-breaches/energetic-bear-under-the-microscope/d/d-id/1297712.

[111] See http://www.defensenews.com/article/20141202/DEFREG04/312020030/Report-Iran-Hackers-Infiltrated-Airlines-Energy-Defense-Firms.

DOCUMENT NO. 6

CYBERSECURITY: ACTIONS NEEDED TO ADDRESS CHALLENGES FACING FEDERAL SYSTEMS

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

United States Government Accountability Office

Testimony Before the Committee on Oversight and Government Reform, House of Representatives,

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, April 22, 2015

GAO-15-573T

GAO
Highlights

Highlights of GAO-15-573T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Federal agencies, as well as their contractors, depend on interconnected computer systems and electronic data to carry out essential mission-related functions. Thus, the security of these systems and networks is vital to protecting national and economic security, public health and safety, and the flow of commerce. If information security controls are ineffective, resources may be lost, information—including sensitive personal information—may be compromised, and the operations of government and critical infrastructure could be disrupted, with potentially catastrophic effects. Federal law sets forth various requirements, roles, and responsibilities for securing federal agencies' systems and information. In addition, GAO has designated federal information security as a high-risk area since 1997.

GAO was asked to provide a statement summarizing cyber threats facing federal agency and contractor systems, and challenges in securing these systems. In preparing this statement, GAO relied on its previously published work in this area.

What GAO Recommends

In its previous work, GAO has made numerous recommendations to agencies to assist in addressing the identified cybersecurity challenges.

For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Federal and contractor systems face an evolving array of cyber-based threats. These threats can be unintentional—for example, from equipment failure, careless or poorly trained employees; or intentional—targeted or untargeted attacks from criminals, hackers, adversarial nations, or terrorists, among others. Threat actors use a variety of attack techniques that can adversely affect federal information, computers, software, networks, or operations, potentially resulting in the disclosure, alteration, or loss of sensitive information; destruction or disruption of critical systems; or damage to economic and national security. These concerns are further highlighted by the sharp increase in cyber incidents reported by federal agencies over the last several years, as well as the reported impact of such incidents on government and contractor systems.

Because of the risk posed by these threats, it is crucial that the federal government take appropriate steps to secure its information and information systems. However, GAO has identified a number of challenges facing the government's approach to cybersecurity, including the following:

- **Implementing risk-based cybersecurity programs at federal agencies:** For fiscal year 2014, 19 of 24 major federal agencies reported that deficiencies in information security controls constituted either a material weakness or significant deficiency in internal controls over their financial reporting. In addition, inspectors general at 23 of these agencies cited information security as a major management challenge for their agency.
- **Securing building and access control systems:** GAO previously reported that the Department of Homeland Security lacked a strategy for addressing cyber risks to agencies' building and access control systems—computers that monitor and control building operations—and that the General Services Administration had not fully assessed the risk of cyber attacks to such systems.
- **Overseeing contractors:** The agencies GAO reviewed were inconsistent in overseeing contractors' implementation of security controls for systems they operate on behalf of agencies.
- **Improving incident response:** The agencies GAO reviewed did not always effectively respond to cybersecurity incidents or develop comprehensive policies, plans, and procedures to guide incident-response activities.

- **Responding to breaches of personally identifiable information:** The agencies GAO reviewed have inconsistently implemented policies and procedures for responding to data breaches involving sensitive personal information.
- **Implementing security programs at small agencies:** Smaller federal agencies (generally those with 6,000 or fewer employees) have not always fully implemented comprehensive agency-wide information security programs.

Until agencies take actions to address these challenges—including the hundreds of recommendations made by GAO and inspectors general—their systems and information will be at increased risk of compromise from cyber-based attacks and other threats.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you for inviting me to testify about cyber threats facing federal information systems at today's hearing. As you know, federal agencies and their contractors are dependent on computerized (cyber) information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. Safeguarding federal computer systems and the systems that support critical infrastructures—referred to as cyber critical infrastructure protection—is a continuing concern. In February 2015, the Director of National Intelligence testified that cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact.[1]

Underscoring the importance of this issue, we have designated federal information security as a high-risk area since 1997 and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. In the 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.[2]

As discussed with your staff, my testimony today will describe (1) cyber threats facing federal and contractor systems and (2) challenges in securing them, as well as actions needed to address these challenges. In preparing this statement in April 2015 we relied on our previous work in these areas.[3] The reports presenting this work contain detailed overviews of its scope and the methodology we used to carry it out. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

[1] James R. Clapper, Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Armed Services Committee (February 26, 2015).

[2] See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[3] See the list of related GAO products at the end of this statement.

Background

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit sensitive and proprietary information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, as well as developing into an extended information and communications infrastructure supporting vital services such as power distribution, health care, law enforcement, and national defense.

Consequently, the security of these systems and networks is essential to protecting national and economic security, public health and safety, and the flow of commerce. Conversely, ineffective information security controls can result in significant risks, including

- loss or theft of computer resources, assets, and funds;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, personally identifiable information (PII),[4] or proprietary business information;
- disruption of critical operations supporting critical infrastructure, national defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government;
- use of computer resources for unauthorized purposes or to launch attacks on other systems;
- damage to networks and equipment; and
- high costs for remediation.

Recognizing the importance of these issues, Congress recently enacted laws intended to improve federal cybersecurity. These include the Federal Information Security Modernization Act of 2014 (FISMA), which revised the Federal Information Security Management Act of 2002 to, among other things, clarify and strengthen information security roles and responsibilities for the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS). The act also reiterated the requirement for federal agencies to develop, document, and implement an agency-wide information security program. The program is to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

[4] Personally identifiable information is information about an individual maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, biometric records, and any other personal information that is linked or linkable to an individual.

In addition, the Cybersecurity Workforce Assessment Act and the Homeland Security Cybersecurity Workforce Assessment Act aim to help DHS address its cybersecurity workforce challenges. Another law, the National Cybersecurity Protection Act of 2014, codifies the role of DHS's National Cybersecurity and Communications Integration Center as the federal civilian interface for sharing information between federal and nonfederal entities regarding cyber risk, incidents, analysis, and warnings. The Cybersecurity Enhancement Act of 2014, among other things, authorizes the National Institute of Standards and Technology (NIST) to facilitate and support the development of voluntary standards to reduce cyber risks to critical infrastructure and to develop and encourage the implementation of a strategy for the use and adoption of cloud computing services by the federal government.

The Federal Government and Its Contractors Face an Evolving Array of Cyber-Based Threats

Risks to cyber-based assets can originate from unintentional and intentional threats. Unintentional threats can be caused by, among other things, defective computer or network equipment, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

Threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. Table 1 describes common sources of cyber threats.

Table 1: Sources of Cybersecurity Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network, or bot-net, of compromised, remotely controlled systems to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized criminal groups use cyber exploits to commit identity theft, online fraud, and computer extortion. International corporate spies and criminal organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers/hacktivists	Hackers break into networks for the challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated actors who use cyber exploits to further political goals. While gaining unauthorized access once required a fair amount of skill or computer knowledge,

Threat source	Description
	hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their position within the organization often allows them to gain unrestricted access and cause damage to the targeted system or to steal system data. The insider threat includes contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to potentially have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his February 2015 testimony, the Director of National Intelligence stated that, among state actors, China, and Russia have highly sophisticated cyber programs, while Iran and North Korea have lesser technical capabilities but possibly more disruptive intent.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, and the Software Engineering Institute's CERT® Coordination Center. | GAO-15-573T

These threat sources make use of various techniques—or exploits—that may adversely affect federal information, computers, software, networks, and operations. Table 2 describes common types of cyber exploits.

Table 2: Types of Cyber Exploits

Type of exploit	Description
Cross-site scripting	An attack that uses third-party web resources to run script within the victim's web browser or scriptable application. This occurs when a browser visits a malicious website or clicks a malicious link. The most dangerous consequences occur when

Type of exploit	Description
	this method is used to exploit additional vulnerabilities that may permit an attacker to steal cookies (data exchanged between a web server and a browser), log key strokes, capture screen shots, discover and collect network information, and remotely access and control the victim's machine.
Denial-of-service/ distributed denial-of-service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources. A distributed denial-of-service attack is a variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Malware	Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples of malware include logic bombs, Trojan Horses, ransomware, viruses, and worms.
Phishing/spear phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information. Spear phishing is a phishing exploit that is targeted to a specific individual or group.
Passive wiretapping	The monitoring or recording of data, such as passwords transmitted in clear text, while they are being transmitted over a communications link. This is done without altering or affecting the data.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malware and other cyber threats.
Spoofing	Creating a fraudulent website to mimic an actual, well-known website run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source.
Structured Query Language (SQL) injection	An attack that involves the alteration of a database search in a web-based application, which can be used to obtain unauthorized access to sensitive information in a database.
War driving	The method of driving through cities and neighborhoods with a wireless-equipped computer–sometimes with a powerful antenna–searching for unsecured wireless networks.
Zero-day exploit	An exploit that takes advantage of a security vulnerability previously unknown to the general public. In many cases, the exploit code is written by the same person who discovered the vulnerability. By writing an exploit for the previously unknown vulnerability, the attacker creates a potent threat since the compressed timeframe between public discoveries of both makes it difficult to defend against.

Source: GAO analysis of data from the National Institute of Standards and Technology, United States Computer Emergency Readiness Team, and industry reports; and GAO. | GAO-15-573T

An adversarial threat source may employ multiple tactics, techniques, and exploits to conduct a cyber attack. NIST has identified several representative events that may constitute a cyber attack:[5]

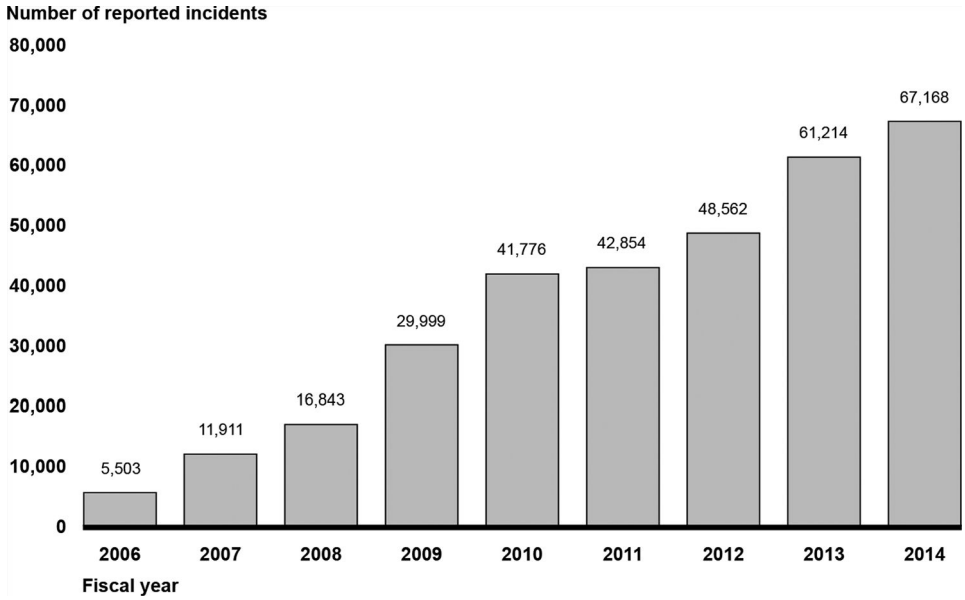
- **Perform reconnaissance and gather information:** An adversary may gather information on a target by, for example, scanning its network perimeters or using publicly available information.
- **Craft or create attack tools:** An adversary prepares its means of attack by, for example, crafting a phishing attack or creating a counterfeit ("spoof") website.
- **Deliver, insert, or install malicious capabilities:** An adversary can use common delivery mechanisms, such as e-mail or downloadable software, to insert or install malware into its target's systems.
- **Exploit and compromise:** An adversary may exploit poorly configured, unauthorized, or otherwise vulnerable information systems to gain access.
- **Conduct an attack:** Attacks can include efforts to intercept information or disrupt operations (e.g., denial of service or physical attacks).
- **Achieve results:** Desired results include obtaining sensitive information via network "sniffing" or exfiltration, causing degradation or destruction of the target's capabilities; damaging the integrity of information through creating, deleting, or modifying data; or causing unauthorized disclosure of sensitive information.
- **Maintain a presence or set of capabilities:** An adversary may try to maintain an undetected presence on its target's systems by inhibiting the effectiveness of intrusion-detection capabilities or adapting behavior in response to the organization's surveillance and security measures.

More generally, the nature of cyber-based attacks can vastly enhance their reach and impact. For example, cyber attacks do not require physical proximity to their victims, can be carried out at high speeds and directed at multiple victims simultaneously, and can more easily allow attackers to remain anonymous. These inherent advantages, combined with the increasing sophistication of cyber tools and techniques, allow threat actors to target government agencies and their contractors, potentially resulting in the disclosure, alteration, or loss of sensitive information, including PII; theft of intellectual property; destruction or disruption of critical systems; and damage to economic and national security.

The number of information security incidents affecting systems supporting the federal government is increasing. Specifically, the number of information security incidents reported by federal agencies to the U.S. Computer Emergency Readiness Team (US-CERT) increased from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent (see fig. 1).

[5] NIST, *Guide for Conducting Risk Assessments*, Special Publication 800-30, Revision 1 (Gaithersburg, Md.: September 2012).

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014

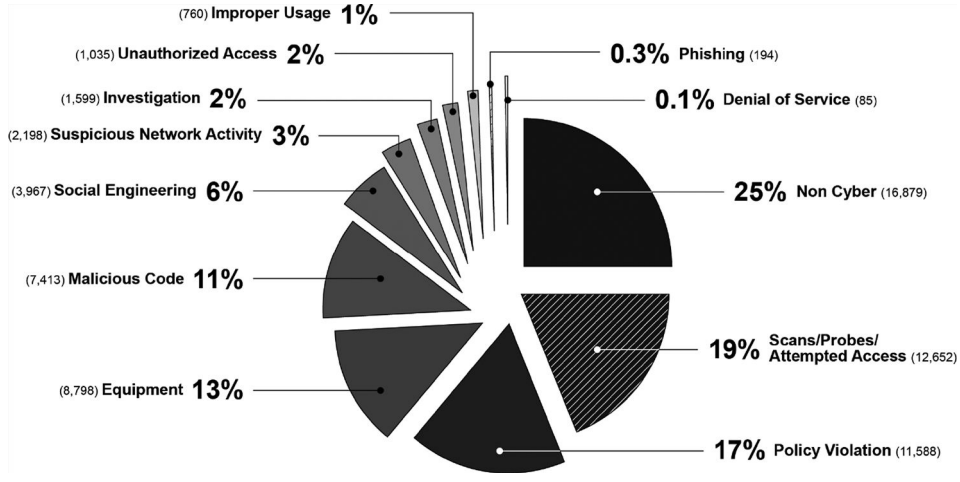


Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006–2014. | GAO-15-573T

Similarly, the number of information security incidents involving PII reported by federal agencies has more than doubled in recent years, from 10,481 in 2009 to 27,624 in 2014.

Figure 2 shows the different types of incidents reported in fiscal year 2014.

Figure 2: Information Security Incidents by Category, Fiscal Year 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-573T

These incidents and others like them could adversely affect national security; damage public health and safety; and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Recent examples highlight the potential impact of such incidents:

- In April 2015, the Department of Veterans Affairs (VA) Office of Inspector General reported that two VA contractors had improperly accessed the VA network from foreign countries using personally owned equipment.
- In September 2014, a cyber intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.
- According to the Director of National Intelligence, unauthorized computer intrusions were detected in 2014 on the networks of the Office of Personnel Management and two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.
- In 2011, according to a media report, the Deputy Secretary of Defense acknowledged a significant cyber attack in which a large number of files was taken by foreign intruders from a defense contractor. The deputy secretary was quoted as saying "it is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies" and that some of the data concerned "our most sensitive systems."

The Federal Government Faces Ongoing Challenges in Its Approach to Cybersecurity

Given the risk posed by cyber threats and the increasing number of incidents, it is crucial that the federal government take appropriate steps to secure its systems and information. However, both we and agency inspectors general have identified challenges in the government's approach to cybersecurity, including those related to protecting the government's information and systems. In particular, challenges remain in the following key areas:

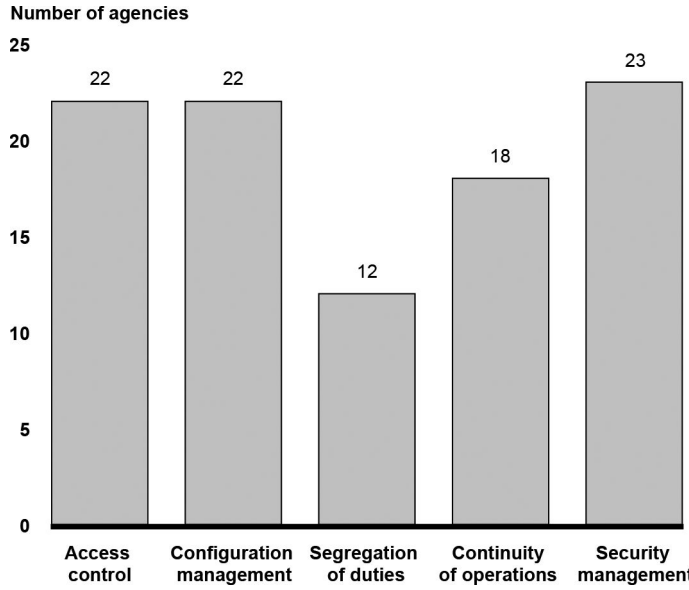
- **Designing and implementing risk-based cybersecurity programs at federal agencies.** Agencies continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results. Specifically, for fiscal year 2014, 19 of the 24 federal agencies covered by the Chief Financial Officers Act[6] reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their financial reporting.[7] Moreover, inspectors general at 23 of the 24 agencies cited information

[6] The 24 CFO Act agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[7] A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

security as a major management challenge for their agency. For fiscal year 2014, most of the agencies had weaknesses in five key security control categories.[8] Figure 3 shows the number of the 24 agencies reviewed with weaknesses in each of the five control categories for fiscal year 2014.

Figure 3: Information Security Weaknesses at 24 Federal Agencies Reviewed for Fiscal Year 2014



Source: GAO analysis of agencies, Inspector General and GAO reports as of April 17, 2015. | GAO-15-573T

Over the last several years, GAO and agency inspectors general have made hundreds of recommendations to agencies aimed at improving their implementation of information security controls. For example:

- **Addressing cybersecurity for building and access control systems.** In December 2014 we reported that DHS lacked a strategy for addressing cyber risk to building and access control systems[9] and that its Interagency Security Committee had not included cyber threats to such systems in its threat report to federal agencies.[10] Further, the General Services Administration (GSA) had not fully assessed the

[8] These control categories are (1) limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide information security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks regularly.

[9] Building and access control systems are computers that monitor and control building operations such as elevators; electrical power; and heating, ventilation, and air conditioning.

[10] GAO, *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems*, GAO-15-6 (Washington, D.C.: Dec. 12, 2014).

risk of cyber attacks aimed at building control systems. We recommended that DHS and GSA take steps to address these weaknesses. DHS and GSA agreed with our recommendations.

- **Enhancing oversight of contractors providing IT services.** In August 2014 we reported that five of six agencies reviewed were inconsistent in overseeing assessments of contractors' implementation of security controls.[11] This was partly because agencies had not documented IT security procedures for effectively overseeing contractor performance. In addition, according to OMB, 16 of 24 agency inspectors general found that their agency's program for managing contractor systems lacked at least one required element. We recommended that OMB, in conjunction with DHS, develop and clarify guidance to agencies for annually reporting the number of contractor-operated systems and that the reviewed agencies establish and implement IT security oversight procedures for such systems. OMB did not comment on our report, but the agencies generally concurred with our recommendations.
- **Improving security incident response activities.** In April 2014 we reported that the 24 major agencies did not consistently demonstrate that they had been effectively responding to cyber incidents.[12] Specifically, we estimated that agencies did not completely document actions taken in response to detected incidents reported in fiscal year 2012 in about 65 percent of cases.[13] In addition, six agencies we reviewed had not fully developed comprehensive policies, plans, and procedures to guide their incident-response activities. We recommended that DHS and OMB address agency incident-response practices government-wide and that the six agencies in our review improve the effectiveness of their cyber incident response programs. The agencies generally agreed with these recommendations.
- **Responding to breaches of PII.** In December 2013 we reported that eight federal agencies had inconsistently implemented policies and procedures for responding to data breaches involving PII.[14] In addition, OMB requirements for reporting PII-related data breaches were not always feasible or necessary. Thus, we concluded that agencies may not be consistently taking actions to limit the risk to individuals from PII-related data breaches and may be expending resources to meet OMB reporting requirements that provide little value. We recommended that OMB revise its guidance on federal agencies' responses to a PII-related data breach and that the reviewed agencies take specific actions to improve their response to PII-related data breaches. OMB neither agreed nor disagreed with our recommendation; four of the reviewed agencies agreed, two partially agreed, and two neither agreed nor disagreed.

[11] GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

[12] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

[13] This estimate was based on a statistical sample of cyber incidents reported in fiscal year 2012, with 95 percent confidence that the estimate falls between 58 and 72 percent.

[14] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

- **Implementing security programs at small agencies.** In June 2014 we reported that six small agencies (i.e., agencies with 6,000 or fewer employees) had not fully implemented their information security programs.[15] For example, key elements of their plans, policies, and procedures were outdated, incomplete, or did not exist, and two of the agencies had not developed an information security program with the required elements. We recommended that OMB include a list of agencies that did not report on the implementation of their information security programs in its annual report to Congress on compliance with the requirements of FISMA, as well as including information on small agencies' programs. We also recommended that DHS develop guidance and services targeted at small agencies. OMB and DHS generally concurred with our recommendations.

Until federal agencies take actions to address these challenges—including implementing the hundreds of recommendations made by us and inspectors general—federal systems and information, as well as sensitive personal information about members of the public, will be at an increased risk of compromise from cyber-based attacks and other threats.

In summary, the cyber threats facing the nation are evolving and growing, with a wide array of threat actors having access to increasingly sophisticated techniques for exploiting system vulnerabilities. The danger posed by these threats is heightened by weaknesses in the federal government's approach to protecting federal systems and information, including personally identifiable information entrusted to the government by members of the public. Implementing GAO's many outstanding recommendations will assist agencies in better protecting their systems and information, which will in turn reduce the risk of the potentially devastating impacts of cyber attacks.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, this concludes my statement. I would be happy to answer any questions you may have.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Larry Crosland (Assistant Director), Rosanna Guerrero, Fatima Jahan, and Lee McCracken.

[15] GAO, *Information Security: Additional Oversight Needed to Improve Programs at Small Agencies*, GAO-14-344, (Washington, D.C.: June 25, 2014).

DOCUMENT NO. 7

CYBERSECURITY: RECENT DATA BREACHES ILLUSTRATE NEED FOR STRONG CONTROLS ACROSS FEDERAL AGENCIES

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

United States Government Accountability Office

Testimony Before the Subcommittee on Cybersecurity,
Infrastructure Protection, and Security Technologies,
Committee on Homeland Security, House of Representatives,

For Release on Delivery
Expected at 2:00 p.m. ET
Wednesday, June 24, 2015

GAO-15-725T

GAO
Highlights

Highlights of GAO-15-725T, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Effective cybersecurity for federal information systems is essential to preventing the loss of resources, the compromise of sensitive information, and the disruption of government operations. Federal information and systems face an evolving array of cyber-based threats, and recent data breaches at federal agencies highlight the impact that can result from ineffective security controls.

Since 1997, GAO has designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. This year, in GAO's high-risk update, the

area was further expanded to include protecting the privacy of personal information that is collected, maintained, and shared by both federal and nonfederal entities.

This statement summarizes (1) challenges facing federal agencies in securing their systems and information and (2) government-wide initiatives, including those led by DHS, aimed at improving cybersecurity. In preparing this statement, GAO relied on its previously published and ongoing work in this area.

What GAO Recommends

In previous work, GAO and agency inspectors general have made hundreds of recommendations to assist agencies in addressing cybersecurity challenges. GAO has also made recommendations to improve government-wide initiatives.

For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

GAO has identified a number of challenges federal agencies face in addressing threats to their cybersecurity, including the following:

- Designing and implementing a risk-based cybersecurity program.
- Enhancing oversight of contractors providing IT services.
- Improving security incident response activities.
- Responding to breaches of personal information.
- Implementing cybersecurity programs at small agencies.

Until federal agencies take actions to address these challenges—including implementing the hundreds of recommendations GAO and agency inspectors general have made—federal systems and information, including sensitive personal information, will be at an increased risk of compromise from cyber-based attacks and other threats.

In an effort to bolster cybersecurity across the federal government, several government-wide initiatives, spearheaded by the Department of Homeland Security (DHS) and the Office of Management and Budget (OMB), are under way. These include the following:

- **Personal Identity Verification:** In 2004, the President directed the establishment of a government-wide standard for secure and reliable forms of ID for federal employees and contractor personnel who access government facilities and systems. Subsequently, OMB directed agencies to issue personal identity verification credentials to control access to federal facilities and systems. OMB recently reported that only 41 percent of user accounts at 23 civilian agencies had required these credentials for accessing agency systems.
- **Continuous Diagnostics and Mitigation:** DHS, in collaboration with the General Services Administration, has established a government-wide contract for agencies to purchase tools that are intended to identify cybersecurity risks on an ongoing basis. These tools can support agencies' efforts to monitor their networks for

security vulnerabilities and generate prioritized alerts to enable agency staff to mitigate the most critical weaknesses. The Department of State adopted a continuous monitoring program, and in 2011 GAO reported on the benefits of the program and challenges the department faced in implementing its approach.

- **National Cybersecurity Protection System (NCPS):** This system, also referred to as EINSTEIN, is to include capabilities for monitoring network traffic and detecting and preventing intrusions, among other things. GAO has ongoing work reviewing the implementation of NCPS, and preliminary observations indicate that implementation of the intrusion detection and prevention capabilities may be limited and DHS appears to have not fully defined requirements for future capabilities.

While these initiatives are intended to improve security, no single technology or tool is sufficient to protect against all cyber threats. Rather, agencies need to employ a multilayered, "defense in depth" approach to security that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee:

Thank you for inviting me to testify at today's hearing on the Department of Homeland Security's (DHS) efforts to secure federal information systems. As you know, the federal government faces an array of cyber-based threats to its systems and data, as illustrated by the recently reported data breaches at the Office of Personnel Management (OPM), which affected millions of current and former federal employees. Such incidents underscore the urgent need for effective implementation of information security controls at federal agencies.

Since 1997, we have designated federal information security as a government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the nation's critical infrastructure. Most recently, in the 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)[1]—that is, personal information that is collected, maintained, and shared by both federal and nonfederal entities.[2]

My statement today will discuss (1) cybersecurity challenges that federal agencies face in securing their systems and information and (2) government-wide initiatives, including those led by DHS, aimed at improving agencies' cybersecurity. In preparing this statement, we relied on our previous work in these areas, as well as the preliminary observations from our ongoing review of DHS's EINSTEIN initiative. We discussed these observations with DHS officials. The prior reports cited throughout this statement contain detailed discussions of the scope of the work and the methodology used to carry it out. All the work on which this statement is based was conducted or is being conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate

[1] Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

[2] See GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As computer technology has advanced, both government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit proprietary and other sensitive information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the Internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, and has developed into an extended information and communications infrastructure that supports vital services such as power distribution, health care, law enforcement, and national defense.

Ineffective protection of these information systems and networks can result in a failure to deliver these vital services, and result in

- loss or theft of computer resources, assets, and funds;
- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as national security information, PII, and proprietary business information;
- disruption of essential operations supporting critical infrastructure, national defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in government;
- use of computer resources for unauthorized purposes or to launch attacks on other systems;
- damage to networks and equipment; and
- high costs for remediation.

Recognizing the importance of these issues, Congress enacted laws intended to improve the protection of federal information and systems. These laws include the Federal Information Security Modernization Act of 2014 (FISMA),[3] which, among other things, authorizes DHS to (1) assist the Office of Management and Budget (OMB) with overseeing and monitoring agencies' implementation of security requirements; (2) operate the federal information security incident center; and (3) provide agencies with operational and technical assistance, such as that for continuously diagnosing and mitigating cyber threats and vulnerabilities. The act also reiterated the 2002 FISMA requirement for the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information or information systems.

[3] The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the very similar Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107-347, Dec. 17, 2002).

In addition, the act requires federal agencies to develop, document, and implement an agency-wide information security program. The program is to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

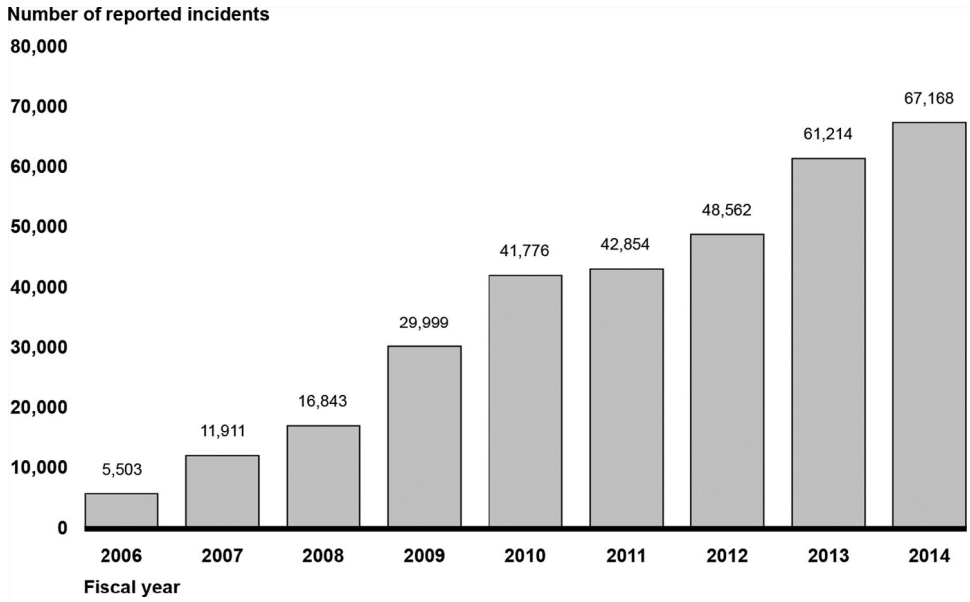
Cyber Threats to Federal Systems

Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. They make use of various techniques—or exploits—that may adversely affect federal information, computers, software, networks, and operations.

Since fiscal year 2006, the number of information security incidents affecting systems supporting the federal government has steadily increased each year: rising from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent (see fig. 1).

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006–2014. | GAO-15-725T

Furthermore, the number of reported security incidents involving PII at federal agencies has more than doubled in recent years—from 10,481 incidents in fiscal year 2009 to 27,624 incidents in fiscal year 2014.

These incidents and others like them can adversely affect national security; damage public health and safety; and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Recent examples highlight the impact of such incidents:

- In June 2015, OPM reported that an intrusion into its systems affected personnel records of about 4 million current and former federal employees. The Director of OPM also stated that a separate incident may have compromised OPM systems related to background investigations, but its scope and impact have not yet been determined.
- In June 2015, the Commissioner of the Internal Revenue Service (IRS) testified that unauthorized third parties had gained access to taxpayer information from its "Get Transcript" application. According to IRS, criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses.
- In April 2015, the Department of Veterans Affairs (VA) Office of Inspector General reported that two VA contractors had improperly accessed the VA network from foreign countries using personally owned equipment.
- In February 2015, the Director of National Intelligence stated that unauthorized computer intrusions were detected in 2014 on OPM's networks and those of two of its contractors. The two contractors were involved in processing sensitive PII related to national security clearances for federal employees.
- In September 2014, a cyber-intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.

Federal Agencies Face Ongoing Cybersecurity Challenges

Given the risks posed by cyber threats and the increasing number of incidents, it is crucial that federal agencies take appropriate steps to secure their systems and information. We and agency inspectors general have identified challenges in protecting federal information and systems, including those in the following key areas:

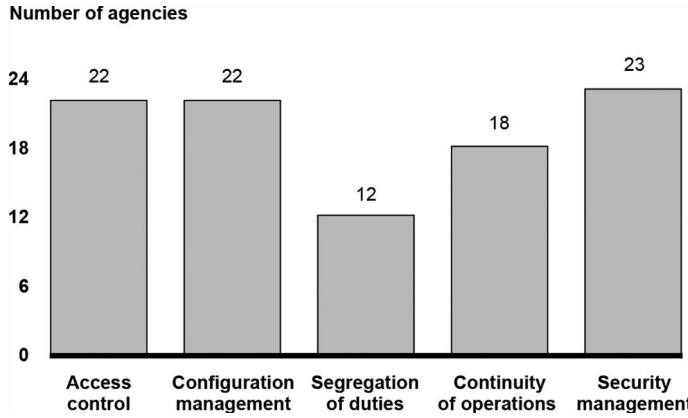
- **Designing and implementing risk-based cybersecurity programs at federal agencies.** Agencies continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results. Specifically, for fiscal year 2014, 19 of the 24 federal agencies covered by the Chief Financial Officers (CFO) Act[4] reported that information security control deficiencies were either

[4] These are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

a material weakness or a significant deficiency in internal controls over their financial reporting.[5] Moreover, inspectors general at 23 of the 24 agencies cited information security as a major management challenge for their agency.

As we testified in April 2015, for fiscal year 2014, most of the agencies had weaknesses in the five key security control categories.[6] These control categories are (1) limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an ongoing basis. (See fig. 2.)

Figure 2: Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014



Source: GAO analysis of agencies, Inspector General and GAO reports as of April 17, 2015. | GAO-15-725T

Examples of these weaknesses include: (1) granting users access permissions that exceed the level required to perform their legitimate job-related functions; (2) not ensuring that only authorized users can access an agency's systems; (3) not using encryption to protect sensitive data from being intercepted and compromised; (4) not updating software with the current versions and latest security patches

[5] A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[6] GAO, *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems*, GAO-15-573T (Washington, D.C.: Apr. 22, 2015).

to protect against known vulnerabilities; and (5) not ensuring employees were trained commensurate with their responsibilities. GAO and agency inspectors general have made hundreds of recommendations to agencies aimed at improving their implementation of these information security controls.

- **Enhancing oversight of contractors providing IT services.** In August 2014, we reported that five of six agencies we reviewed were inconsistent in overseeing assessments of contractors' implementation of security controls.[7] This was partly because agencies had not documented IT security procedures for effectively overseeing contractor performance. In addition, according to OMB, 16 of 24 agency inspectors general determined that their agency's program for managing contractor systems lacked at least one required element. We recommended that OMB, in conjunction with DHS, develop and clarify guidance to agencies for annually reporting the number of contractor-operated systems and that the reviewed agencies establish and implement IT security oversight procedures for such systems. OMB did not comment on our report, but the agencies generally concurred with our recommendations.
- **Improving security incident response activities.** In April 2014, we reported that the 24 agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[8] Specifically, we estimated that agencies had not completely documented actions taken in response to detected incidents reported in fiscal year 2012 in about 65 percent of cases.[9] In addition, the 6 agencies we reviewed had not fully developed comprehensive policies, plans, and procedures to guide their incident response activities. We recommended that OMB address agency incident response practices government-wide and that the 6 agencies improve the effectiveness of their cyber incident response programs. The agencies generally agreed with these recommendations. We also made two recommendations to DHS concerning government-wide incident response practices. DHS concurred with the recommendations and, to date, has implemented one of them.
- **Responding to breaches of PII.** In December 2013, we reported that eight federal agencies had inconsistently implemented policies and procedures for responding to data breaches involving PII.[10] In addition, OMB requirements for reporting PII-related data breaches were not always feasible or necessary. Thus, we concluded that agencies may not be consistently taking actions to limit the risk to individuals from PII-related data breaches and may be expending resources to meet OMB reporting requirements that provide little value. We recommended that OMB revise its guidance to agencies on responding to a PII-related data breach and that the reviewed agencies take specific actions to improve their response to PII-related data breaches. OMB neither agreed nor disagreed with our recommendation; four

[7] GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls*, GAO-14-612 (Washington, D.C.: Aug. 8, 2014).

[8] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

[9] This estimate was based on a statistical sample of cyber incidents reported in fiscal year 2012, with 95 percent confidence that the estimate falls between 58 and 72 percent.

[10] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*, GAO-14-34 (Washington, D.C.: Dec. 9, 2013).

of the reviewed agencies agreed, two partially agreed, and two neither agreed nor disagreed.

- **Implementing security programs at small agencies.** In June 2014, we reported that six small agencies (i.e., agencies with 6,000 or fewer employees) had not implemented or not fully implemented their information security programs.[11] For example, key elements of their plans, policies, and procedures were outdated, incomplete, or did not exist, and two of the agencies had not developed an information security program with the required elements. We recommended that OMB include a list of agencies that did not report on the implementation of their information security programs in its annual report to Congress on compliance with the requirements of FISMA, and include information on small agencies' programs. OMB generally concurred with our recommendations. We also recommended that DHS develop guidance and services targeted at small agencies. DHS has implemented this recommendation.

Until federal agencies take actions to address these challenges—including implementing the hundreds of recommendations we and inspectors general have made—federal systems and information will be at an increased risk of compromise from cyber-based attacks and other threats.

Government-Wide Cybersecurity Initiatives Present Potential Benefits and Challenges

In addition to the efforts of individual agencies, DHS and OMB have several initiatives under way to enhance cybersecurity across the federal government. While these initiatives all have potential benefits, they also have limitations.

Personal Identity Verification: In August 2004, Homeland Security Presidential Directive 12 ordered the establishment of a mandatory, government-wide standard for secure and reliable forms of identification for federal government employees and contractor personnel who access government-controlled facilities and information systems. Subsequently, the National Institute of Standards and Technology (NIST) defined requirements for such personal identity verification (PIV) credentials based on "smart cards"—plastic cards with integrated circuit chips to store and process data—and OMB directed federal agencies to issue and use PIV credentials to control access to federal facilities and systems.

In September 2011, we reported that OMB and the eight agencies in our review had made mixed progress for using PIV credentials for controlling access to federal facilities and information systems.[12] We attributed this mixed progress to a number of obstacles, including logistical problems in issuing PIV credentials to all agency personnel and agencies not making this effort a priority. We made several recommendations to the eight agencies and to OMB to more fully implement PIV card capabilities. Although two agencies did not comment, seven agencies agreed with our recommendations or discussed actions they were taking to address them. For example, we made four

[11] GAO, *Information Security: Additional Oversight Needed to Improve Programs at Small Agencies*, GAO-14-344 (Washington, D.C.: June 25, 2014).

[12] GAO, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*, GAO-11-751 (Washington, D.C.: Sept. 20, 2011).

recommendations to DHS, who concurred and has taken action to implement them. In February 2015, OMB reported that, as of the end of fiscal year 2014, only 41 percent of agency user accounts at the 23 civilian CFO Act agencies required PIV cards for accessing agency systems.[13]

Continuous Diagnostics and Mitigation (CDM): According to DHS, this program is intended to provide federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These tools include sensors that perform automated searches for known cyber vulnerabilities, the results of which feed into a dashboard that alerts network managers. These alerts can be prioritized, enabling agencies to allocate resources based on risk. DHS, in partnership with the General Services Administration, has established a government-wide contract that is intended to allow federal agencies (as well as state, local, and tribal governmental agencies) to acquire CDM tools at discounted rates.

In July 2011, we reported on the Department of State's (State) implementation of its continuous monitoring program, referred to as iPost.[14] We determined that State's implementation of iPost had improved visibility over information security at the department and helped IT administrators identify, monitor, and mitigate information security weaknesses. However, we also noted limitations and challenges with State's approach, including ensuring that its risk-scoring program identified relevant risks and that iPost data were timely, complete, and accurate. We made several recommendations to improve the implementation of the iPost program, and State partially agreed.

National Cybersecurity Protection System (NCPS): The National Cybersecurity Protection System, operationally known as "EINSTEIN," is a suite of capabilities intended to detect and prevent malicious network traffic from entering and exiting federal civilian government networks. The EINSTEIN capabilities of NCPS are described in table 1.[15]

Table 1: National Cybersecurity Protection System EINSTEIN Capabilities

Operational name	Capability intended	Description
EINSTEIN 1	Network Flow	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their Internet connections.[a]
EINSTEIN 2	Intrusion Detection	Monitors federal agency Internet connections for specific predefined signatures of known malicious activity and alerts US-CERT when specific network activity matching the predetermined signatures is detected.[b]

[13] OMB, *Annual Report to Congress: Federal Information Security Management Act* (Washington, D.C.: Feb. 27, 2015).

[14] GAO, *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain, GAO-11-149* (Washington, D.C.: July 8, 2011)

[15] In addition to the EINSTEIN capabilities listed in table 1, NCPS also includes a set of capabilities related to analytics and information sharing.

Operational name	Capability intended	Description
EINSTEIN 3 Accelerated	Intrusion Prevention	Automatically blocks malicious traffic from entering or leaving federal civilian executive branch agency networks. This capability is managed by Internet service providers, who administer intrusion prevention and threat-based decision-making using DHS-developed indicators of malicious cyber activity to develop signatures.[c]

Source: GAO analysis of DHS documentation and prior GAO reports. | GAO-15-725T

[a] The network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

[b] Signatures are recognizable, distinguishing patterns associated with cyber attacks such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

[c] An indicator is defined by DHS as human-readable cyber data used to identify some form of malicious cyber activity. These data may be related to Internet Protocol addresses, domains, e-mail headers, files, and character strings. Indicators can be either classified or unclassified.

In March 2010, we reported that while agencies that participated in EINSTEIN 1 improved their identification of incidents and mitigation of attacks, DHS lacked performance measures to understand if the initiative was meeting its objectives.[16] We made four recommendations regarding the management of the EINSTEIN program, and DHS has since taken action to address them.

Currently, we are reviewing NCPS, as mandated by Congress. The objectives of our review are to determine the extent to which (1) NCPS meets stated objectives, (2) DHS has designed requirements for future stages of the system, and (3) federal agencies have adopted the system.

Our final report is expected to be released later this year, and our preliminary observations include the following:

- DHS appears to have developed and deployed aspects of the intrusion detection and intrusion prevention capabilities, but potential weaknesses may limit their ability to detect and prevent computer intrusions. For example, NCPS detects signature anomalies using only one of three detection methodologies identified by NIST (signature-based, anomaly-based, and stateful protocol analysis). Further, the system has the ability to prevent intrusions, but is currently only able to proactively mitigate threats across a limited subset of network traffic (i.e., Domain Name System traffic and e-mail).
- DHS has identified a set of NCPS capabilities that are planned to be implemented in fiscal year 2016, but it does not appear to have developed formalized requirements for capabilities planned through fiscal year 2018.

[16] GAO, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies*, GAO-10-237 (Washington, D.C.: Mar. 12, 2010).

- The NCPS intrusion detection capability appears to have been implemented at 23 CFO Act agencies.[17] The intrusion prevention capability appears to have limited deployment, at portions of only 5 of these agencies. Deployment may have been hampered by various implementation and policy challenges.

In conclusion, the danger posed by the wide array of cyber threats facing the nation is heightened by weaknesses in the federal government's approach to protecting its systems and information. While recent government-wide initiatives hold promise for bolstering the federal cybersecurity posture, it is important to note that no single technology or set of practices is sufficient to protect against all these threats. A "defense in depth" strategy is required that includes well-trained personnel, effective and consistently applied processes, and appropriately implemented technologies. While agencies have elements of such a strategy in place, more needs to be done to fully implement it and to address existing weaknesses. In particular, implementing GAO and inspector general recommendations will strengthen agencies' ability to protect their systems and information, reducing the risk of a potentially devastating cyber attack.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions you may have.

Contact and Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other staff members who contributed to this statement include Larry Crosland and Michael Gilmore (assistant directors), Bradley Becker, Christopher Businsky, Nancy Glover, Rosanna Guerrero, Kush Malhotra, and Lee McCracken.

[17] The Department of Defense is not required to implement EINSTEIN.

DOCUMENT NO. 8

CYBERWARFARE AND CYBERTERRORISM: IN BRIEF

CRS Report R43955

Catherine A. Theohary
Specialist in National Security Policy and Information Operations

John W. Rollins
Specialist in Terrorism and National Security

March 27, 2015

Summary

Recent incidents have highlighted the lack of consensus internationally on what defines a cyberattack, an act of war in cyberspace, or cyberterrorism. Cyberwar is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. Cyberterrorism can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies. Within each of these categories, different motivations as well as overlapping intent and methods of various actors can complicate response options.

Criminals, terrorists, and spies rely heavily on cyber-based technologies to support organizational objectives. Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives. Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. Cyberthieves are individuals who engage in illegal cyberattacks for monetary gain. Cyberwarriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives. Cyberactivists are individuals who perform cyberattacks for pleasure, philosophical, political, or other nonmonetary reasons.

There are no clear criteria yet for determining whether a cyberattack is criminal, an act of hactivism, terrorism, or a nation-state's use of force equivalent to an armed attack. Likewise, no international, legally binding instruments have yet been drafted explicitly to regulate inter-state relations in cyberspace.

The current domestic legal framework surrounding cyberwarfare and cyberterrorism is equally complicated. Authorizations for military activity in cyberspace contain broad and undefined terms. There is no legal definition for cyberterrorism. The USA PATRIOT Act's definition of terrorism and references to the Computer Fraud and Abuse Act appear to be the only applicable working construct. Lingering ambiguities in cyberattack categorization and response policy have caused some to question whether the United States has an effective deterrent strategy in place with respect to malicious activity in cyberspace.

Introduction

"Cyberattack" is a relatively recent term that can refer to a range of activities conducted through the use of information and communications technology (ICT). The use of distributed denial of service (DDoS) attacks has become a widespread method of achieving political ends through the disruption of online services. In these types of attacks, a server is overwhelmed with Internet traffic so access to a particular website is degraded or denied. The advent of the Stuxnet worm, which some consider the first cyberweapon, showed that cyberattacks may have a more destructive and lasting effect. Appearing to target Iran, Stuxnet malware attacked the computerized industrial control systems on which nuclear centrifuges operate, causing them to self-destruct.

Recent international events have raised questions on when a cyberattack could be considered an act of war, and what sorts of response options are available to victim nations. Although there is no clear doctrinal definition of "cyberwarfare," it is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. Cyberterrorism can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and response is typically the jurisdiction of law enforcement agencies.

The cyberattacks on Sony Entertainment illustrate the difficulties in categorizing attacks and formulating a response policy. On November 24, 2014, Sony experienced a cyberattack that disabled its information technology systems, destroyed data and workstations, and released internal emails and other materials. Warnings surfaced that threatened "9/11-style" terrorist attacks on theaters scheduled to show the film *The Interview*, causing some theaters to cancel screenings and for Sony to cancel its widespread release, although U.S. officials claimed to have "no specific, credible intelligence of such a plot." The Federal Bureau of Investigation (FBI) and the Director of National Intelligence (DNI) attributed the cyberattacks to the North Korean government; North Korea denied involvement in the attack, but praised a hacktivist group, called the "Guardians of Peace," for having done a "righteous deed." During a December 19, 2014, press conference, President Obama pledged to "respond proportionally" to North Korea's alleged

cyber assault, "in a place, time and manner of our choosing." President Obama referred to the incident as an act of "cyber-vandalism," while others decried it as an act of cyberwar.

This incident illustrates challenges in cyberattack categorization, particularly with respect to the actors involved and their motivations as well as issues of sovereignty regarding where the actors were physically located. With the globalized nature of the Internet, perpetrators can launch cyberattacks from anywhere in the world and route the attacks through servers of third-party countries. Was the cyberattack on Sony, a private corporation with headquarters in Japan, an attack on the United States? Further, could it be considered an act of terrorism, a use of force, or cybercrime? In categorizing the attacks on Sony as an act of "cyber vandalism," which typically includes defacing websites and is usually the realm of politically motivated actors known as "hacktivists," President Obama raised questions of what type of response could be considered "proportional," and against whom. Another potential policy question could be the circumstances under which the United States would commit troops to respond to a cyberattack. Related to this is the question of whether the U.S. has an effective deterrence strategy in place. According to DNI Clapper, "If they get global recognition at a low cost and no consequence, they will do it again and keep doing it again until we push back."[1]

The Cyberwarfare Ecosystem: A Variety of Threat Actors

Criminals, terrorists, and spies rely heavily on cyber-based technologies to support organizational objectives. Commonly recognized cyber-aggressors and representative examples of the harm they can inflict include the following:

Cyberterrorists are state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives. Transnational terrorist organizations, insurgents, and jihadists have used the Internet as a tool for planning attacks, radicalization and recruitment, a method of propaganda distribution, and a means of communication, and for disruptive purposes.[2] While no unclassified reports have been published regarding a cyberattack on a critical component of U.S. infrastructure, the vulnerability of critical life-sustaining control systems being accessed and destroyed via the Internet has been demonstrated. In 2009, the Department of Homeland Security (DHS) conducted an experiment that revealed some of the vulnerabilities to the nation's control systems that manage power generators and grids. The experiment, known as the Aurora Project, entailed a computer-based attack on a power generator's control system that caused operations to cease and the equipment to be destroyed.[3] Cyberterrorists may be seeking a destructive capability to exploit these vulnerabilities in critical infrastructure.

[1] See http://www.bloomberg.com/politics/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony.

[2] For additional information, see CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson.

[3] See "Challenges Remain in DHS' Efforts to Security Control Systems," Department of Homeland Security, Office of Inspector General, August 2009. For a discussion of how computer code may have caused the halting of operations at an Iranian nuclear facility see CRS Report R41524, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, by Paul K. Kerr, John W. Rollins, and Catherine A. Theohary.

Cyberspies are individuals who steal classified or proprietary information used by governments or private corporations to gain a competitive strategic, security, financial, or political advantage. These individuals often work at the behest of, and take direction from, foreign government entities. Targets include government networks, cleared defense contractors, and private companies. For example, a 2011 FBI report noted, "a company was the victim of an intrusion and had lost 10 years' worth of research and development data—valued at $1 billion—virtually overnight."[4] Likewise, in 2008 the Department of Defense's (DOD) classified computer network system was unlawfully accessed and "the computer code, placed there by a foreign intelligence agency, uploaded itself undetected onto both classified and unclassified systems from which data could be transferred to servers under foreign control."[5]

Cyberthieves are individuals who engage in illegal cyberattacks for monetary gain. Examples include an organization or individual who illegally accesses a technology system to steal and use or sell credit card numbers and someone who deceives a victim into providing access to a financial account. One estimate has placed the annual cost of cybercrime to individuals in 24 countries at $388 billion.[6] However, given the complex and sometimes ambiguous nature of the costs associated with cybercrime, and the reluctance in many cases of victims to admit to being attacked, there does not appear to be any publicly available, comprehensive, reliable assessment of the overall costs of cyberattacks.

Cyberwarriors are agents or quasi-agents of nation-states who develop capabilities and undertake cyberattacks in support of a country's strategic objectives.[7] These entities may or may not be acting on behalf of the government with respect to target selection, timing of the attack, and type(s) of cyberattack and are often blamed by the host country when accusations are levied by the nation that has been attacked. Often, when a foreign government is provided evidence that a cyberattack is emanating from its country, the nation that has been attacked is informed that the perpetrators acted of their own volition and not at the behest of the government. In August 2012 a series of cyberattacks were directed against Saudi Aramco, the world's largest oil and gas producer. The attacks compromised 30,000 computers and the code was apparently designed to disrupt or halt oil production. Some security officials have suggested that Iran may have supported this attack. However, numerous groups, some with links to nations with objectives counter to Saudi Arabia, have claimed credit for this incident.

Cyberactivists are individuals who perform cyberattacks for pleasure, philosophical, political, or other nonmonetary reasons. Examples include someone who attacks a technology system as a personal challenge (who might be termed a "classic" hacker),

[4] Executive Assistant Director Shawn Henry, *Responding to the Cyber Threat*, Federal Bureau of Investigation, Baltimore, MD, 2011.

[5] Department of Defense Deputy Secretary of Defense William J. Lynn III, "Defending a New Domain," Foreign Affairs, October 2010.

[6] For discussions of federal law and issues relating to cybercrime, see CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*, by Charles Doyle, and CRS Report R41927, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement*, by Kristin Finklea.

[7] For additional information, see CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary.

and a "hacktivist" such as a member of the cyber-group Anonymous who undertakes an attack for political reasons. The activities of these groups can range from nuisance-related denial of service attacks and website defacement to disrupting government and private corporation business processes.

The threats posed by these cyber-aggressors and the types of attacks they can pursue are not mutually exclusive. For example, a hacker targeting the intellectual property of a corporation may be categorized as both a cyberthief and a cyberspy. A cyberterrorist and cyberwarrior may be employing different technological capabilities in support of a nation's security and political objectives. Some reports indicate that cybercrime has now surpassed the illegal drug trade as a source of funding for terrorist groups, although there is some confusion as to whether a particular action should be categorized as cybercrime.[8] Ascertaining information about an aggressor and its capabilities and intentions is difficult.[9] The threats posed by these aggressors coupled with the United States' proclivity to be an early adopter of emerging technologies,[10] which are often interdependent and contain vulnerabilities, makes for a complex environment when considering operational responses, policies, and legislation designed to safeguard the nation's strategic economic and security interests.

Cyberwarfare

There are no clear criteria yet for determining whether a cyberattack is criminal, an act of hactivism, terrorism, or a nation-state's use of force equivalent to an armed attack. Likewise, no international, legally binding instruments have yet been drafted explicitly to regulate inter-state relations in cyberspace. In September 2012, the State Department took a public position on whether cyber activities could constitute a use of force under Article 2(4) of the U.N. Charter and customary international law. According to State's then-legal advisor, Harold Koh, "Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force."[11] Examples offered in Koh's remarks included triggering a meltdown at a nuclear plant, opening a dam and causing flood damage, and causing airplanes to crash by interfering with air traffic control. By focusing on the ends achieved rather than the means with which they are carried out, this definition of cyberwar fits easily within existing international legal frameworks. If an actor employs a cyberweapon to produce kinetic effects that might

[8] Lillian Ablon, Martin C. Libicki, Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar,* RAND. For more information on cybercrime definitions, see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*, by Kristin Finklea and Catherine A. Theohary.

[9] The concept of attribution in the cyber world entails an attempt to identify with some degree of specificity and confidence the geographic location, identity, capabilities, and intention of the cyber-aggressor. Mobile technologies and sophisticated data routing processes and techniques often make attribution difficult for U.S. intelligence and law enforcement communities.

[10] Emerging cyber-based technologies that may be vulnerable to the actions of a cyber-aggressor include items that are in use but not yet widely adopted or are currently being developed. For additional information on how the convergence of inexpensive, highly sophisticated, and easily accessible technology is providing opportunities for cyber-aggressors to exploit vulnerabilities found in a technologically laden society see *Global Trends 2030: Alternative Worlds, National Intelligence Council*, Office of the Director of National Intelligence, December 10, 2012.

[11] Remarks of Harold Hongju Koh, Legal Advisor U.S. Department of State, at a USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, September 18, 2012.

warrant fire power under other circumstances, then the use of that cyberweapon rises to the level of the use of force.

However, the United States recognizes that cyberattacks without kinetic effects are also an element of armed conflict under certain circumstances. Koh explained that cyberattacks on information networks in the course of an ongoing armed conflict would be governed by the same principles of proportionality that apply to other actions under the law of armed conflict. These principles include retaliation in response to a cyberattack with a proportional use of kinetic force. In addition, "computer network activities that amount to an armed attack or imminent threat thereof" may trigger a nation's right to self-defense under Article 51 of the U.N. Charter. Koh cites in his remarks the 2011 *International Strategy for Cyberspace*,[12] which affirmed that "when warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country." The *International Strategy* goes on to say that the U.S. reserves the right to use all means necessary—diplomatic, informational, military, and economic—as appropriate and consistent with applicable law, and exhausting all options before military force whenever possible.

Rules of the Road and Norm-Building in Cyberspace

One of the defense objectives of the *International Strategy for Cyberspace* is to work internationally "to encourage responsible behavior and oppose those who would seek to disrupt networks and systems, dissuading and deterring malicious actors, and reserving the right to defend national assets." A growing awareness of the threat environment in cyberspace has led to two major international processes geared toward developing international expert consensus among international cyber authorities.

A year after the 2007 DDoS attack on Estonia, NATO established the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn, Estonia. The CCDCOE hosts workshops and courses on law and ethics in cyberspace, as well as cyber defense exercises. In 2009, the center convened an international group of independent experts to draft a manual on the law governing cyberwarfare. The *Tallinn Manual*, as it is known, was published in 2013.[13] It sets out 95 "black letter rules" governing cyber conflict addressing sovereignty, state responsibility, the law of armed conflict, humanitarian law, and the law of neutrality. The *Tallinn Manual* is an academic text: although it offers reasonable justifications for the application of international law, it is non-binding and the authors stress that they do not speak for NATO or the CCDCOE.

In the provisions of Article 5 of the North Atlantic Treaty, an attack on one member is considered an attack on all, affording military assistance in accordance with Article 51 of the United Nations Charter. However, NATO does not presently define cyberattacks as clear military action. The *Tallinn Manual* equates a use of force to those cyber operations whose "effects . . . were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack." Article 4 of the North Atlantic Treaty applies the principles of collective consultation to any member state whose security and

[12] *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[13] Tallinn Manual on the International Law Applicable to Cyber Warfare, available at https://ccdcoe.org/tallinn-manual.html.

territorial integrity has been threatened; however it is unclear how this would apply to the various categories of cyberattacks, some of which may not have kinetic equivalents. If an attack is deemed to be orchestrated by a handful of cyber criminals, whether politically or financially motivated, then it may fall upon the attacked state to determine the appropriate response within its jurisdiction. However the transnational nature of most criminal organizations in cyberspace can complicate decisions of jurisdiction.

Law of Armed Conflict

Reprisals for armed attacks are permitted in international law when a belligerent violates international law during peacetime, or the law of armed conflict during wartime. However, the term "armed attack" has no legal definition and is still open to interpretation with respect to cyberattacks. The so-called "Law of War," also known as the law of armed conflict, embodied in the Geneva and Hague Conventions and the U.N. Charter may in some circumstances apply to cyberattacks, but without attempts by nation states to apply it, or specific agreement on its applicability, its relevance remains unclear. It is also complicated by difficulties in attribution, the potential use of remote computers, and possible harm to third parties from cyber counterattacks, which may be difficult to contain. In addition, questions of territorial boundaries and what constitutes an armed attack in cyberspace remain. The law's application would appear clearest in situations where a cyberattack causes physical damage, such as disruption of an electric grid. As mentioned above, the *Tallinn Manual* addresses many of these questions.[14] In the absence of a legal definition for what constitutes an "armed attack" in cyberspace, Professor Michael Schmitt has proposed criteria for analysis under international law:[15]

Severity: Perhaps the most significant factor in the analysis, consequences involving physical harm to individuals or property will alone amount to a use of force while those generating only minor inconvenience or irritation will not. The more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force.

Immediacy: The sooner consequences manifest, the less opportunity states have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, states harbor a greater concern about immediate consequences than those that are delayed or build slowly over time.

Directness: The greater the attenuation between the initial act and the resulting consequences, the less likely states will be to deem the actor responsible for violating the prohibition on the use of force.

---

[14] For a detailed discussion, see Hathaway et al., "The Law of Cyber-Attack." See also CRS Report R43848, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, by Catherine A. Theohary; James A. Lewis, *Conflict and Negotiation in Cyberspace* (Center for Strategic and International Studies, February 2013), https://csis.org/files/publication/130208_Lewis_ConflictCyberspace_Web.pdf; Mary Ellen O'Connell and Louise Arimatsu, *Cyber Security and International Law* (London, UK: Chatham House, May 29, 2012), http://www.tsa.gov/sites/default/files/assets/pdf/Intermodal/pipeline_sec_incident_recvr_protocol_plan.pdf.

[15] This section has been adapted from M.N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revised", Vol. 56 *Villanova Law Review* 2011, at p. 576 *et seq.*; M. N. Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context" and K Ziolkowski, "Ius ad bellum in Cyberspace—Some Thoughts on the 'Schmitt-Criteria' for Use of Force" in the 2012 4th *International Conference on Cyber Conflict*, C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)

Invasiveness: The more secure a targeted system, the greater the concern as to its penetration. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas in combat the forces of one state cross into another in violation of its sovereignty. Although highly invasive, espionage does not constitute a use of force (or armed attack) under international law absent a nonconsensual physical penetration of the target state's territory.

Measurability: The more quantifiable and identifiable a set of consequences, the more a state's interest will be deemed to have been affected. This is particularly challenging in a cyber event, where damage, economic or otherwise, is difficult to quantify. Economic coercion or hardship does not qualify under international law as an armed attack.

Presumptive legitimacy: In international law, acts which are not forbidden are permitted; absent an explicit prohibition, an act is presumptively legitimate. For instance, it is generally accepted that international law governing the use of force does not prohibit propaganda, psychological warfare, or espionage. To the extent such activities are conducted through cyber operations, they are presumptively legitimate.

Responsibility: The law of state responsibility governs when a state will be responsible for cyber operations. However that responsibility lies along a continuum from operations conducted by a state itself to those in which it is merely involved in some fashion. The closer the nexus between a state and the operations, the more likely other states will be inclined to characterize them as uses of force, for the greater the risk posed to international stability. Attributing the level of state involvement to a cyberattack can be particularly challenging.

The basic principles encompassed in the Hague Conventions regarding the application of Armed Forces are those of military necessity, proportionality, humanity and chivalry. If a nation's military is conducting cyber operations according to these principles, it may be said to be engaging in cyberwar.

Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime[16] is the first international treaty to attempt to harmonize laws across countries as to what constitutes criminal activity in the cyber realm. This law enforcement treaty, also known as the Budapest Convention, requires signatories to adopt criminal laws against specified types of activities in cyberspace, to empower law enforcement agencies to investigate such activities, and to cooperate with other signatories. While widely cited as the most substantive international agreement relating to cybersecurity, some observers regard it as unsuccessful.[17] Critics warn that the Convention is short on the enforcement side, and lacks jurisdiction in countries where criminals operate freely. In addition to most members of the Council of Europe, the United States and three other nations have ratified the treaty.[18]

[16] See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[17] Jack Goldsmith, "Cybersecurity Treaties: A Skeptical View" *Future Challenges Essay*, June 2, 2011, http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf. He cites "vague definitions," reservations by signatories, and loopholes as reasons for its lack of success.

[18] Council of Europe, "Convention on Cybercrime, CETS No. 185," accessed February 18, 2013, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG. See also Michael Vatis, "The Council of Europe Convention on Cybercrime," in Proceedings of a Workshop on Deterring

United Nations General Assembly Resolutions

A series of U.N. General Assembly resolutions relating to cybersecurity have been adopted over the past 15 years. One resolution called for the convening of and a report from an international group of government experts from 15 nations, including the United States. The stated purpose of this process was to build "cooperation for a peaceful, secure, resilient and open ICT environment" by agreeing upon "norms, rules and principles of responsible behaviour by States" and identifying confidence and capacity-building measures, including for the exchange of information. Unlike the work done at Tallinn under the auspices of NATO, this U.S.-led process included both China and Russia. The resulting 2010 report, sometimes referred to as the Group of Governmental Experts (GGE) Report, recommended a series of steps to "reduce the risk of misperception resulting from ICT[19] disruptions" but did not incorporate any binding agreements.[20] Nevertheless, some observers believe the report represents progress in overcoming differences between the United States and Russia about various aspects of cybersecurity.[21] In December 2001, the General Assembly approved Resolution 56/183, which endorsed the World Summit on the Information Society (WSIS) to discuss information society opportunities and challenges. This summit was first convened in Geneva, in 2003, and then in Tunis, in 2005, and a10-year follow-on in Geneva in May 2013. Delegates from 175 countries took part in the first summit, where they adopted a Declaration of Principles—a road map for achieving an open information society. The Geneva summit left other, more controversial issues unresolved, including the question of Internet governance and funding. At both summits, proposals for the United States to relinquish control of the Internet Corporation for Assigned Names and Numbers (ICANN) were rejected.

An international treaty banning cyberwarfare and/or information weapons has been proposed in the United Nations by Russian and German delegations. Preferring a normative approach over an arms control styled regime, the United States may wish to reserve its right to develop technologies for countermeasures and reconnaissance against potential cyber foes, particularly those acting outside the boundaries of a state system.

International Telecommunications Regulations

The International Telecommunication Union (ITU) regulates international telecommunications through binding treaties and regulations and nonbinding standards. Regulations prohibit interference with other nations' communication services and

CyberAttacks: Informing Strategies and Developing Options for U.S. Policy (Washington, DC: National Academies Press, 2010), pp. 207–223.

[19] The abbreviation ICT, which stands for information and communications technologies, is increasingly used instead of IT, (information technologies) because of the convergence of telecommunications and computer technology.

[20] United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, July 30, 2010, http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201.

[21] Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review 100*, no. 4 (2012), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.

permit control of non-state telecommunications for security purposes. The regulations do not, however, expressly forbid military cyberattacks. Also, ITU apparently has little enforcement authority.[22]

The ITU convened the World Conference on International Telecommunications (WCIT) in Dubai, United Arab Emirates, during December 3–14, 2012, to review the International Telecommunications Regulations. In the run-up to the summit, many security observers expressed concern over the closed nature of the talks and feared a shift of Internet control away from private entities such as ICANN toward the United Nations and national governments. Although these concerns proved to be largely baseless, a controversial deep packet inspection proposal from the People's Republic of China was adopted at the summit.[23] Dissenting countries, including Germany, fear that this recommendation will result in accelerated Internet censorship in repressed nations.

Other International Law

Some bodies of international law, especially those relating to aviation and the sea, may be applicable to cybersecurity; for example by prohibiting the disruption of air traffic control or other conduct that might jeopardize aviation safety.[24] Bilaterally, mutual legal assistance treaties between countries may be applicable for cybersecurity forensic investigations and prosecution.

The United States has signed at least 16 treaties and other agreements with 13 other countries and the European Union that include information security, classified military information, or defense-related information assurance and protection of computer networks. According to news reports, the United States and Australia have agreed to include cybersecurity cooperation within a defense treaty, declaring that a cyberattack on one country would result in retaliation by both.[25]

Cyberterrorism

As with cyberwarfare, there is no consensus definition of what constitutes cyberterrorism. The closest in law is found in the USA PATRIOT Act 18 U.S.C. 2332b's definition of "acts of terrorism transcending national boundaries" and reference to some activities and damage defined in the Computer Fraud and Abuse Act (CFA) 18 U.S.C. 1030a-c. A notable aspect of this act is its discussion of the "punishment for an offense" entails fines or imprisonment and suggests the offending party is undertaking a criminal act rather than an act of terrorism, which some argue is an act of war if undertaken by a state actor. The CFA is written in such a manner that it could be applied to an individual or groups.

---

[22] Hathaway et al.,"The Law of Cyber-Attack." See also Anthony Rutkowski, "Public International Law of the International Telecommunication Instruments: Cyber Security Treaty Provisions Since 1850," Info 13, no. 1 (2011): 13–31, http://www.emeraldinsight.com/journals.htm?issn=1463-6697&volume=13&issue=1&articleid=1893240& show=pdf&PHPSESSID=9r0c5maa4spkkd9li78ugbjee3.

[23] Deep packet inspection allows the content of a unit of data to be examined as it travels through an inspection point, a process that enables data mining and eavesdropping programs.

[24] Hathaway et al.,"The Law of Cyber-Attack."

[25] See, for example, Lolita Baldor, "Cyber Security Added to US-Australia Treaty," Security on NBCNews.com, 2011, http://www.msnbc.msn.com/id/44527648/ns/technology_and_science-security/t/cyber-security-added-us-australia-treaty/.

18 U.S.C. 1030(a)(1) finds it illegal for an entity to "knowingly access a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data . . . with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation." As noted in this section, it appears this statute only pertains to U.S. government networks or networks that may contain restricted data. There is not yet a precedent for an unauthorized computer-supported intrusion rising to the level of being described as a cyberattack.

Some legal analyses define cyberterrorism as "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives."[26] The USA PATRIOT Act's definition of "federal crime of terrorism" and reference to the CFA seem to follow this definition. However, these provisions are also criminal statutes and generally refer to individuals or organizations rather than state actors. Naval Post Graduate School defense analyst Dorothy Denning's definition of cyber terrorism focuses on the distinction between destructive and disruptive action.[27] Terrorism generates fear comparable to that of physical attack, and is not just a "costly nuisance."[28] Though a DDoS attack itself does not yield this kind of fear or destruction, the problem is the potential for second or third order effects. For example, if telecommunications and emergency services had been completely dismantled in a time of crisis, the effects of that sort of infrastructure attack could potentially be catastrophic. If an attack on the emergency services system had coincided with a planned real-world, kinetic event, cyber terror or even a Cyber Pearl Harbor event may be an appropriate metaphor. However in this case, the emergency service system itself is most likely not a target, but rather the result of collateral damage to a vulnerable telecommunications network.

There are a number of reasons that may explain why the term "cyberterrorism" has not been statutorily defined, including the difficulty in identifying the parameters of what should be construed applicable activities, whether articulating clear redlines would demand a response for lower-level incidents, and retaining strategic maneuverability so as not to bind future U.S. activities in cyberspace.

Use of the Military: Offensive Cyberspace Operations

The War Powers Resolution, P.L. 93-148, 87 Stat. 555, sometimes referred to as the War Powers Act, sets the conditions under which the President may exercise his authority as Commander in Chief of U.S. military forces. First, the Resolution stipulates that it be exercised only pursuant to a declaration of war, specific statutory authorization from Congress, or a national emergency created by an attack upon the United States

[26] http://www.nato.int/structur/library/bibref/cyberterrorism.pdf.

[27] Dorothy E. Denning. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy" http://www.nautilus.org/info-policy/workshop/papers/denning.html.

[28] Serge Krasavin PhD, "What is Cyber-terrorism?," http://www.crime-research.org/library/Cyber-terrorism.htm.

(50 U.S.C. 1541). Second, the Resolution requires the President to consult with Congress before introducing U.S. Armed Forces into hostilities or situations where hostilities are imminent, and to continue such consultations as long as U.S. Armed Forces remain in such situations (50 U.S.C. 1542). Third, it mandates reporting requirements that the President must comply with any time he introduces U.S. Armed Forces into existing or imminent hostilities (50 U.S.C. 1543). Lastly, 50 U.S.C. 1544(b) requires that U.S. forces be withdrawn from hostilities within 60 days of the time a report is submitted or is required to be submitted under 50 U.S.C. 1543(a)(1), unless Congress acts to approve continued military action, or is physically unable to meet as a result of an armed attack upon the United States.

Title 10 of the *United States Code* is the authority under which the military organizes, trains and equips its forces for national defense. Section 954 of the National Defense Authorization Act for Fiscal Year 2012 affirms that "the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict and the War Powers Resolution." The House version (H.R. 1540) contained a provision in Section 962 that would have clarified that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to the Authorization for the Use of Military Force (P.L. 107-40; title 50 United States Code, section 1541 note) outside of the United States or to defend against a cyberattack on an asset of the Department of Defense. Section 941of the House version (H.R. 4310) of the National Defense Authorization Act for Fiscal Year 2013 would have again affirmed the Secretary of Defense's authority to conduct military activities in cyberspace. In particular, it would have clarified that the Secretary of Defense has the authority to conduct clandestine cyberspace activities in support of military operations pursuant to a congressionally authorized use of force outside of the United States, or to defend against a cyberattack on an asset of the DOD. This provision was not in the final version (P.L. 112-239), but a requirement for the Secretary of Defense to provide quarterly briefings to the House and Senate Armed Services Committee on all offensive and significant defensive military operations remained in Section 939.

Another relevant authority through which troops may be dispatched resides in Title 50 of the U.S. Code. Under Title 50, a "covert action" is subject to presidential finding and Intelligence Committee notification requirements. 50 U.S.C. 3093 allows the President to authorize the conduct of a covert action if he determines such an action is necessary to support identifiable foreign policy objectives of the United States and is important to the U.S. national security, which determination shall be set forth in a finding that shall be in writing, "unless immediate action by the United States is required and time does not permit the preparation of a written finding, in which case a written record of the President's decision shall be contemporaneously made and shall be reduced to a written finding as soon as possible but in no event more than 48 hours after the decision is made."

50 U.S.C. 413b(e) defines "covert action" as "activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." The definition then lists certain exclusions. Traditional military activity, although

undefined, is an explicit exception to the covert action definition in 50 U.S.C. 413 as the identity of the sponsor of a traditional military activity may be well known.

According to the Joint Explanatory Statement of the Committee of Conference, H.R. 1455, July 25, 1991, traditional military activities

> include activities by military personnel under the direction and control of a United States military commander (whether or not the U.S. sponsorship of such activities is apparent or later to be acknowledged) preceding and related to hostilities which are either anticipated (meaning approval has been given by the National Command Authorities for the activities and or operational planning for hostilities) to involve U.S. military forces, or where such hostilities involving United States military forces are ongoing, and, where the fact of the U.S. role in the overall operation is apparent or to be acknowledged publicly.

Multiple press sources have reported on a Pentagon plan for "the creation of three types of Cyber Mission Forces under the Cyber Command: 'national mission forces' to protect computer systems that undergird electrical grids, power plants and other infrastructure deemed critical to national and economic security; 'combat mission forces' to help commanders abroad plan and execute attacks or other offensive operations; and 'cyber protection forces' to fortify the Defense Department's networks."[29] These multiservice Cyber Mission Forces numbered under 1,000 in 2013, when DOD announced plans to expand them to roughly 5,000 soldiers and civilians. The target number has since grown to 6,200, with a deadline at the end of FY2016. In early September 2014, a report was provided to Congress from DOD that reportedly stated, "additional capability may be needed for both surge capacity for the [Cyber Mission Forces] and to provide unique and specialized capabilities" for a whole-of-government and nation approach to security in cyberspace.[30]

Author Contact Information

Catherine A. Theohary
Specialist in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844

John W. Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

[29] Seehttp://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

[30] http://www.defensenews.com/article/20141103/TRAINING/311030018/As-cyber-force-grows-manpower-details-emerge.

D. THE EFFICACY OF SANCTIONS IN AVOIDING HYBRID WARFARE AND DETERRING GRAY ZONE THREATS

COMMENTARY

by
Douglas C. Lovelace, Jr.

In Section D of this volume we turn our attention briefly to an increasingly observed aspect of hybrid warfare—the use of sanctions to shape adversary behavior in ways that enhance U.S. security. The first document is a May 2015 Government Accountability Office Report to the Chairman of the Committee on Foreign Affairs of the House of Representatives, entitled *Nonproliferation: State Should Minimize Reporting Delays That May Affect Sanctions on Trade with Iran, North Korea, and Syria*. This report provides unique insights into an area one might not immediately associate with hybrid warfare and Gray Zone threats. It involves the monitoring, reporting, and sanctioning of individuals who transfer prohibited items to states the United States suspects of pursuing or knows are pursuing weapons of mass destruction. The report specifically addresses North Korea, a known nuclear power. It also addresses Iran and Syria, believed to be aspiring nuclear powers.

While the GAO report focuses on the failure of the U.S. Department of State to report illicit transfers in a sufficiently timely manner to allow effective sanctions against those making the transfers, it concurrently exposes a category of hybrid warfare participants that does not immediately come to mind. In doing so, the report gives the reader an appreciation for the diverse players in the mix and how they greatly complicate a unified U.S. strategic approach to waging hybrid warfare, in which many actions take place in the Gray Zone.

The second document in this section on the role of sanctions in hybrid warfare focuses on the challenge posed by North Korea. It is a May 2015 GAO Report to the Chairman of the Senate Committee on Foreign Relations, entitled *North Korea Sanctions: United States Has Increased Flexibility to Impose Sanctions, but United Nations Is Impeded by a Lack of Member State Reports*. We include this document to apprise the reader of the difficulty in imposing sanctions effectively, the reduced efficacy of sanctions when imposed by a single state or small group of states even if the United States is a member, and the variability of sanctions effectiveness depending on the government against which the sanctions are directed.

For North Korea, the imposition of sanctions by the United States appears to have done little to modify the behavior of the rogue regime. Although the international community widely condemns many of North Korea's actions, especially its nuclear weapons

and missile programs, unity of effort in bringing about change that enhances international security is wanting. As the GAO report suggests, many countries are not even reporting the sanctions they have in effect, much less the impact they are having, if any. Although the United States enforces and reports on its stringent sanctions, it remains frustrated by North Korea's leadership. The population of a country ruled by fear of a brutally iron fist is not likely to rise up to force its government to change course in order to have sanctions removed. Therefore, while sanctions are a weapon to be wielded in hybrid warfare, their efficacy is highly suspect.

DOCUMENT NO. 9

NONPROLIFERATION: STATE SHOULD MINIMIZE REPORTING DELAYS THAT MAY AFFECT SANCTIONS ON TRADE WITH IRAN, NORTH KOREA, AND SYRIA

United States Government Accountability Office

Report to the Chairman, Committee on Foreign Affairs, House of Representatives

May 2015

GAO-15-519

GAO
Highlights

Highlights of GAO-15-519, a report to Chairman, Committee on Foreign Affairs, House of Representatives

Why GAO Did This Study

The United States uses sanctions to curb weapons of mass destruction proliferation. Under INKSNA, the President is required every 6 months to provide reports to two congressional committees that identify every foreign person for whom there is credible information that the person has transferred certain items to or from Iran, North Korea, or Syria. INKSNA authorizes the President to impose sanctions on the identified person and requires him to provide justification to the two committees if sanctions are not imposed. The President has delegated this authority to State. State's Deputy Secretary makes determinations about whether to impose sanctions.

GAO was asked to review State's INKSNA implementation. This report (1) examines State's timeliness in providing INKSNA reports, (2) reviews State's reporting process, and (3) identifies the potential impact of its reporting timeliness on the imposition of sanctions.

GAO analyzed data and met with officials from the Departments of State, Defense, and Energy, and met with officials from the Department of Commerce.

What GAO Recommends

GAO recommends that the Secretary of State reconsider State's INKSNA process to ensure that it (1) complies with INKSNA's 6-month reporting cycle, and (2) minimizes delays in its ability to opt to impose sanctions. State concurred with the recommendation but expressed concerns about the difficulty of conducting its process. The GAO report highlights some process efficiencies that State should consider.

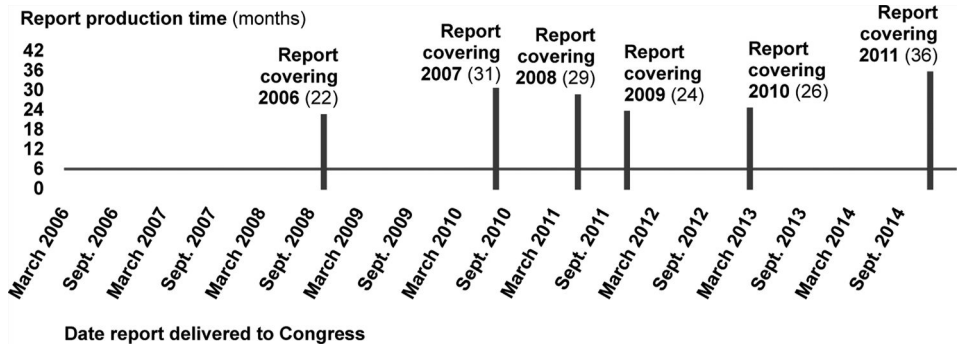
For more information, contact Thomas Melito at (202) 512-9601 or melitot@gao.gov.

What GAO Found

The Department of State (State) is not providing reports to congressional committees in accordance with the 6-month reporting requirements of the 2006 Iran, North Korea, and Syria Nonproliferation Act (INKSNA). Since 2006, it has provided six reports covering a 6-year period (2006 through 2011), instead of 18 reports covering a 9-year period (2006 through 2014), as required by INKSNA. State provided these six reports at irregular intervals averaging 16 months. It provided its most recent report in December 2014, 22 months after it had provided the prior report.

State has not established a process that would allow it to comply with the 6-month reporting cycle required by INKSNA. It uses a complex and lengthy process that involves multiple interagency and internal reviews. Because it processes cases in calendar-year groups, State delays providing a report to the committees until it has resolved all concerns and determined whether to impose sanctions for each transfer in the group. It begins preparing a new report every December, regardless of whether it has completed all previous reports, with the result that State officials sometimes work on several reports simultaneously and may delay work on one report to work on another. State required nearly 3 years to prepare its December 2014 report on transfers that first came to its attention in 2011. Officials told GAO that negotiations and relations with countries can delay the process and assessing transfers in annual groups reduces prospects for confusion among the parties involved in the process (see figure).

State's Delays in Reporting on Transfers and Acquisitions Reportable under INKSNA, 2006–2014



Source: GAO analysis of State data | GAO-15-519

By not complying with INKSA's 6-month reporting cycle, State may have limited its ability to minimize delays in choosing to impose INKSNA sanctions. INKSNA requires State to identify foreign persons in a report before opting to impose sanctions on them. As a result, State did not impose INKSNA sanctions on 23 persons for 2011 transfers until December 2014, when it provided its report addressing 2011 transfers. While officials told GAO that threats of possible sanctions can deter questionable transfers, prolonged delays in eventually imposing potential INKSNA sanctions could erode the credibility of such threats and INKSNA's utility as a tool in helping to curb weapons of mass destruction proliferation associated with Iran, Syria, and North Korea.

Abbreviations

Commerce	Department of Commerce
D	Office of the Deputy Secretary of State
DOD (JCS)	Department of Defense (Joint Chiefs of Staff)
DOD (OSD)	Department of Defense (Office of the Secretary of Defense)
DOE	Department of Energy
H	State Bureau of Legislative Affairs
HFAC	House Committee on Foreign Affairs
IC	Intelligence Community
INA	Iran Nonproliferation Act of 2000
INKSNA	Iran, North Korea, and Syria Nonproliferation Act
IPC	Interagency Policy Committee
ISN	State Bureau of International Security and Nonproliferation
ISN/MBC	State Bureau of International Security and Nonproliferation/State Office of Missile, Biological, and Chemical Nonproliferation
ISNA	Iran and Syria Nonproliferation Act
MBC	State Office of Missile, Biological, and Chemical Nonproliferation
NSC	National Security Council
SFRC	Senate Committee on Foreign Relations
State	Department of State
Treasury	Department of the Treasury
WMD	weapons of mass destruction

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

May 22, 2015

The Honorable Edward R. Royce
Chairman
Committee on Foreign Affairs
House of Representatives

Dear Mr. Chairman:

The advent of global terrorism has heightened concerns about the threat of proliferation of weapons of mass destruction (WMD) and missiles. The United States uses export control regimes and sanctions to combat proliferation by restricting exports of sensitive goods, services, and technologies and to punish those persons that violate such restrictions.[1] It imposes WMD-related sanctions under legal authorities that include the Iran, North Korea, and Syria Nonproliferation Act (INKSNA).[2]

INKSNA requires the President to transmit a report to the Senate Committee on Foreign Relations and the House Committee on Foreign Affairs every 6 months in which she or he identifies foreign persons for which there is credible information indicating they have transferred to, or acquired from, Iran, North Korea, or Syria certain WMD or conventional or missile-related items.[3] INKSNA also authorizes the President to impose sanctions on foreign persons identified in the reports. If the President chooses not to do so, the President must notify the committees and include a written justification that supports the decision not to sanction. The President has delegated INKSNA authorities to the Department of State. The Deputy Secretary of State is responsible for making sanctions determinations, and authorizing delivery to the two cognizant congressional committees.

Because of concerns regarding the timeliness of State's provision of INKSNA reports to the committees, you asked us to review State's implementation of INKSNA. This report (1) examines State's timeliness in providing INKSNA reports, (2) reviews State's reporting process, and (3) identifies the potential impact of State's reporting timeliness on its imposition of sanctions.

---

[1] For purposes of the Iran, North Korea, and Syria Nonproliferation Act (INKSNA), a "person" is (1) a natural person that is an alien; (2) a corporation, business association, partnership, society, trust, or any other nongovernmental entity, organization, or group, that is organized under the laws of a foreign country or has its principal place of business in a foreign country; (3) any foreign government, including any foreign governmental entity; and (4) any successor, subunit, or subsidiary of any entity described above, including any entity in which any entity described in any such subparagraph owns a controlling interest.

[2] Iran, North Korea, and Syria Nonproliferation Act (Pub. L. No. 106-178, §§ 1-7, 114 Stat. 38, Mar. 14, 2000 [codified as amended at 50 U.S.C. § 1701 note]). Congress amended the Iran Nonproliferation Act of 2000 (INA) to include transactions involving Syria in 2005, and amended the Iran and Syria Nonproliferation Act (ISNA) to include transactions involving North Korea in 2006.

[3] These items include goods, services, or technology listed on four multilateral export control regimes and one treaty (see table 1), as well as other goods, services, or technology having the potential to make a material contribution to the development of nuclear, biological, chemical, or conventional weapons, or of ballistic or cruise missile systems.

To address these objectives, we reviewed INKSNA and related legislation. We also obtained and analyzed Department of State data on report publication dates and processing timelines and assessed relevant documents from the Departments of State, Defense, and Energy. In addition, we interviewed officials involved in the INKSNA process from the Departments of State, Energy, Defense, and Commerce. Appendix I provides a detailed description of our scope and methodology.

We conducted this performance audit from September 2014 to May 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

INKSNA requires the President to provide reports on March 14 and September 14 of each year to the Senate Committee on Foreign Relations and the House Committee on Foreign Affairs, in which he or she identifies every foreign person for whom there is credible information that the person has transferred to or from Iran, North Korea, or Syria certain goods, services, or technologies mostly those controlled through four multilateral export control regimes and one treaty.[4] Table 1 provides details on the purpose and items restricted in each one.[5]

Table 1: Purpose and Control Items or Activities Restricted by the Four Multilateral Export Control Regimes and the Treaty Referenced in the Iran, North Korea, and Syria Nonproliferation Act (INKSNA)

Regime/treaty (member states)	**Purpose**	**Controlled items or activities**
Nuclear Suppliers Group Guidelines **(48)**	To ensure that nuclear trade for peaceful purposes does not contribute to the proliferation of nuclear weapons or explosive devices while not unjustly hindering such trade and cooperation	The export of nuclear and nuclear-related dual-use items[a]

[4] The committee report accompanying the bill that became the Iran Nonproliferation Act of 2000 stated that "credible information" was intended to be a very low evidentiary standard—information that is sufficiently believable that a reasonable person would conclude that there is a substantial possibility that a transfer has occurred (H. R. Rep. 106-315, at 65 (Sept. 14, 1999).

[5] Multilateral export control arrangements are referred to as "regimes" and are voluntary, nonbinding arrangements among like-minded supplier countries that aim to restrict trade in sensitive technologies to peaceful purposes. See GAO, Nonproliferation: Strategy Needed to Strengthen Multilateral Export Control Regimes, GAO-03-93, (Washington, D.C.: October 25, 2002).

Regime/treaty (member states)	**Purpose**	**Controlled items or activities**
Missile Technology Control Regime **(34)**	To limit the risks of proliferation of weapons of mass destruction (WMD) (i.e., nuclear, chemical, and biological weapons), by controlling transfers that could make a contribution to delivery systems (other than manned aircraft) for such weapons	Transfer of missiles, rockets, and unmanned air vehicles capable of delivering WMDs, and related equipment, software, and technology
Wassenaar Arrangement list of Dual Use Goods and Technologies and Munitions **(41)**	To contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations	Trade in conventional weapons and related items with dual-use (military and civilian) applications
Australia Group **(42)**	To ensure that the industries of the participating countries do not assist, either purposefully or inadvertently, states seeking to acquire a chemical and biological weapons capability	Trade in 1. chemical weapons precursors; 2. dual-use chemical manufacturing facilities and equipment, and related technology and software; 3. dual-use biological equipment and related technology and software; 4. Human and animal pathogens and toxins; 5. Plant pathogens.
Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction **(190)**	A treaty to outlaw the production, stockpiling, and use of chemical weapons and their precursors, including toxic chemicals and precursors listed in Schedule One or Schedule Two of the convention	Chemical weapons and their precursors

Sources: GAO, Nonproliferation: Strategy Needed to Strengthen Multilateral Export Control Regimes, GAO-03-43 (Washington, D.C.: Oct. 25, 2002), and websites for each of the regimes and treaty. | GAO-15-519

[a] Dual-use items within the Nuclear Suppliers Group guidelines are those that can make a major contribution to an unsafeguarded nuclear fuel cycle or nuclear explosive activity, but which have non-nuclear uses as well.

In addition to these controlled items, INKSNA also includes a category of reportable items for goods, services, or technology, on a case-by-case basis, have the potential to make a material contribution to the development of nuclear, biological, conventional, or chemical weapons, or of ballistic or cruise missile systems.[6] According to State officials, INKSNA's broad list of reportable transfers and acquisitions and discretionary authority to impose sanctions provide the U.S. government an important and flexible tool to achieve its nonproliferation objectives and sanctioning capabilities found in no other U.S. law.[7] INKSNA's scope includes any transfers to or from Iran on or after January 1, 1999; Syria on or after January 1, 2005; and North Korea on or after January 1, 2006.

INKSNA also authorizes the President to apply a range of measures against any foreign person the President has identified in a report he or she has provided to the congressional committees. The measures include (1) a prohibition on U.S. government procurement of goods or services from the person and a ban on imports of products produced by that person, except to the extent the Secretary of State otherwise may determine; (2) a prohibition on U.S. government provision of assistance, except to the extent the Secretary of State otherwise may determine; (3) a prohibition on U.S. government sales of any item on the U.S. Munitions List, and the termination of any ongoing sales of any defense articles, defense services, or design and construction services controlled under the Arms Export Control Act; and (4) that new licenses will be denied, and any existing licenses suspended, for transfers of items controlled under the Export Administration Act of 1979 or the Export Administration Regulations. Once imposed, INKSNA sanctions are in effect for 2 years at State's discretion.

In addition, INKSNA requires the President to notify the congressional committees of his or her rationale for not imposing sanctions against foreign persons identified in the report. Under INKSNA, the President cannot apply sanctions to reported persons if he or she finds that (1) the person did not "knowingly transfer to or acquire from Iran, North Korea, or Syria" reportable items; (2) the goods, services, or technology "did not materially contribute to the efforts of Iran, North Korea or Syria, as the case may be, to develop nuclear, biological, or chemical weapons, or ballistic or cruise missile systems, or weapons listed on the Wassenaar Arrangement Munitions List," (3) the person is subject to the jurisdiction of a government that is an adherent to "one or more relevant nonproliferation regimes" and the transfer was consistent with such regime's guidelines; or (4) the government of jurisdiction "has imposed meaningful penalties" on the identified person.

The President has delegated INKSNA authorities to State. The Deputy Secretary of State exercises this authority by making sanctions determinations, and authorizing delivery of INKSNA reports to the committees. State arranges to have the names of the foreign persons deemed to have engaged in the sanctioned transfers or acquisitions published in the *Federal Register* soon after it delivers the reports to the committees.

[6] According to State, the act of one or more foreign persons transferring to or acquiring from another person or persons goods, services, or technologies potentially reportable under IKSNA in a single transaction constitutes one transfer. A case consists of the information the U.S. government has compiled related to each transfer in the process of determining whether or not the transfer is reportable.

[7] While the U.S. government could use other nonproliferation authorities to sanction (some) transfers identified in its INKSNA reports, most of these other sanctions authorities require judgments as to the end use of the item; these judgments are not part of INKSNA reporting requirements.

From 2006 to May 2015, State imposed sanctions on 82 foreign persons under INKSNA deemed to have engaged in reportable transfers to or acquisitions from Iran, North Korea, and Syria, primarily on persons located in China, Iran, Syria, and Sudan (see table 2). Seventeen of these foreign persons had INKSNA sanctions imposed on them more than once.

Table 2: Location of Foreign Persons Sanctioned under the Iran, North Korea, and Syria Nonproliferation Act (INKSNA), by Date

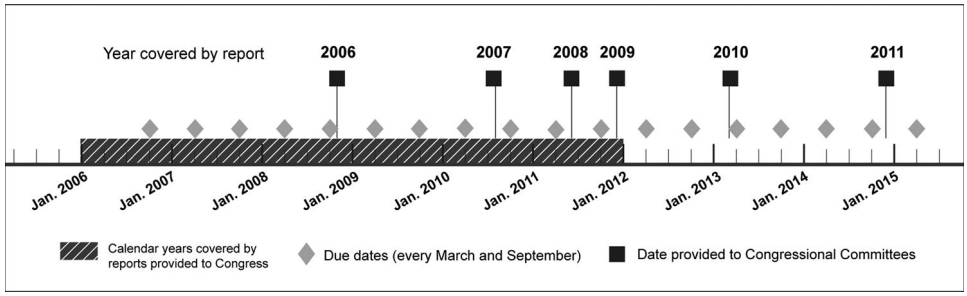
	Calendar year of report (effective date of sanctions)						
Location of foreign persons	**2006 (10/23/08)**	**2007 (7/14/10)**	**2008 (5/23/11)**	**2009 (12/20/11)**	**2010 (2/5/13)**	**2011 (12/19/14)**	**Total**
China	3	4	4	3	5	3	22
Iran	1	2	6	2	3	3	17
Syria	1		2	1	1	5	10
Sudan	2				2	5	9
Belarus		1	2	1	2	1	7
North Korea	2	1	1	1		1	6
Russia	1					4	5
Other	3		1		1	1	6
Total	**13**	**8**	**16**	**8**	**14**	**23**	**82**

Source: GAO analysis of Department of State data. | GAO-15-519

State Is Not Providing Reports to Congressional Committees Every 6 Months as Required by INKSNA

State is not providing reports to the two cognizant congressional committees in accordance with INKSNA's 6-month reporting requirements. Since 2006, it has provided six reports covering a 6-year period (2006 through 2011), instead of 18 reports covering a 9-year period (2006 through 2014), as required by INKSNA. If State had submitted a report every 6 months during this 6-year period as required by law, they would have produced 11 reports. Instead, each of the six reports covered a period spanning an entire calendar year and focused on transfers that first came to State's attention in one of the six calendar years occurring between 2006 and 2011(see fig. 1). State provided these six reports at irregular intervals that have averaged 16 months, ranging between 7 and 22 months apart. It provided its most recent report in December 2014, 22 months after its previous report. The interval between the last two reports was the longest interval between reports since the beginning of 2006.

Figure 1: Timeliness of State's INKSNA Reports, 2006–2015



Source: GAO analysis of State data | GAO-15-519

State Has Not Established a Process That Allows It to Comply with INKSNA's Required 6-Month Reporting Cycle

State has not established a process that would allow it to comply with the 6-month reporting cycle required by INKSNA. State uses a complex and lengthy process that involves multiple interagency and internal reviews to compile credible information about a group of reportable transfers that first came to its attention in a single calendar year, and to determine whether to impose sanctions on foreign persons associated with those transfers. Because its process focuses on a group of transfers that came to its attention in a single year, State delays providing a report to the committees until it has resolved concerns it may have regarding any of the transfers in the group covered in the report and determined whether to sanction persons associated with any of those transfers. State officials begin preparing a new report every December, regardless of whether they have completed and provided all previous reports. State officials have told GAO they sometimes must delay work on one draft report to work on another, and that they can make only a limited amount of progress toward completing a new report before they have completed earlier reports. According to State, they use this approach because each report builds on the previous installment, including any determinations to defer a decision on sanctions and any determinations on whether to add nonlisted items to reportability on a case-by-case basis. As a result, State required almost 3 years to prepare its December 2014 report, which addressed transfers that first came to its attention in 2011.

State Uses a Complex Process Involving Multiple Interagency and Internal Reviews

According to officials in the office responsible for producing the report— State's Bureau of International Security and Nonproliferation's Office of Missile, Biological, and Chemical Nonproliferation (ISN/MBC)—State's process for implementing INKSNA consists of the12 following steps, as depicted interactively in figure 2 and described in appendix II.

Figure 2: State's INKSNA Process

[Editor's Note: Because Figure 2 is an interactive graphic, it cannot be reproduced in print; please see Appendix II, where the INKSNA Process is explained.]

State officials told us that while the four State-led interagency working groups (named in figure 2 above) meet on a regular basis to evaluate reporting from a wide variety of sources on transfers and flag activity that might trigger INKSNA or other legal authorities, State typically begins the report preparation process, starting with compiling the activity for the draft report, once the relevant calendar year ends.[8] The State Bureau of International Security and Nonproliferation/State Office of Missile, Biological, and Chemical Nonproliferation (ISN/MBC), working with other agencies and the Intelligence Community, compiles a list of transfers that first came to its working groups' attention during the previous calendar year and then provides the list along with any diplomatic histories associated with each transfer to the Intelligence Community for fact checking and to determine whether the names of the foreign persons associated with the transfers are releasable to the *Federal Register* if State imposes sanctions. State then distributes the corrected package of transfers and any other information to the relevant interagency working group that includes the other federal departments involved in this process—the Department of Defense (DOD), the Department of Energy (DOE), and the Department of Commerce (DOC). Next, State chairs an interagency Policy Committee meeting (held at the deputy assistant secretary or office director level), where State and other members of the interagency working groups provide advice on whether each transfer is reportable under INKSNA and whether it should result in sanctions. This meeting is followed by reviews by State officials in geographic and functional bureaus.[9]

ISN/MBC includes the result of these reviews in an action memo that it sends to the Deputy Secretary of State for the final determination as to which transfers to include in the report and which persons to sanction in connection with those transfers.[10] Following the Deputy Secretary's determinations, State officials prepare the final version of the report, transmit it to the cognizant congressional committees, and arrange to have sanctions notices published in the *Federal Register*.

State's Process Requires on Average More than 2 Years to Complete a Report

Using this process, State has required, on average, more than 2 years to produce each of the six INKSNA reports that it provided to the cognizant congressional committees between 2006 and 2015. It required almost 3 years to complete the report it provided

[8] The working groups also examine intelligence to identify proliferation-related shipments that the United States seeks to interdict, some of which may also be reportable under INKSNA.

[9] Examples of such bureaus include Economic and Business Affairs, Near Eastern Affairs, and East Asian and Pacific Affairs.

[10] State also may take other actions, such as sending notices (démarches) or cables alerting countries where the sanctioned entities reside or are located.

to the committees in December 2014 covering calendar year 2011. Our analysis of the production times of State's six INKSNA reports indicates that the three longest stages of State's process involve State's compilation of potential reportable transfers into a single list (steps 1 and 2); State's scheduling and holding of the sub-Interagency Policy Committee meeting (held at the deputy assistant secretary or office director level) to discuss the transfers (steps 4 and 5); and the Deputy Secretary's review of the action memo in making his or her determinations (steps 8 and 9). For example, concerning the report State provided in December 2014, the Deputy Secretary required more than a year to review the action memo for transfers State learned of in 2011 and to determine which persons to identify in the report and whether to apply sanctions.

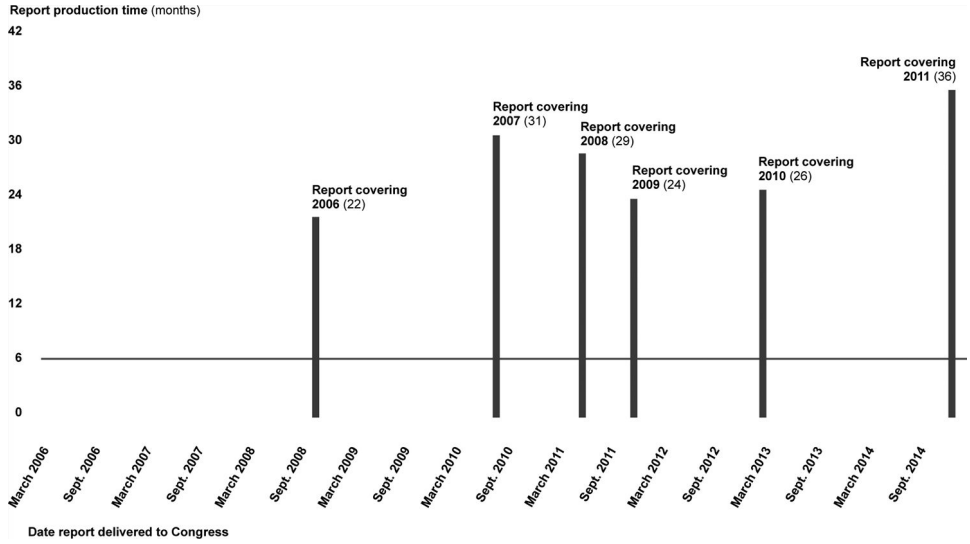
State officials told us that a variety of political concerns, such as international negotiations and relations with countries involved in transfers, can delay State's INKSNA process. They stated that these concerns can particularly delay the steps that involve internal State approvals, including the Deputy Secretary's review and sanctions determination.

State's practice of focusing each report on a group of transfers that first came to its attention in a single calendar year also contributes to the length of time State's process requires to complete a report. State does not provide a report to the congressional committees until it has resolved concerns it may have about every one of the transfers in the group covered in the report and determined whether to impose sanctions on persons associated with each of the transfers in that group. As a result, a single problematic case in a group can delay State's provision of the report, which may include other INKSNA-reportable transfers that State may be otherwise ready to report to Congress.

As a result of this practice of focusing each report on a single year's group of transfers and acquisitions, State officials must either complete a report within a year or manage the preparation of a backlog of multiple reports, each covering a different calendar year and each in a different stage of State's process. Under State's process, State officials begin preparing a new report every December, regardless of whether they have completed and provided all previous reports. State data indicate that State officials were simultaneously processing three reports, covering calendar years 2011, 2012, and 2013, in the last 6 months of 2014. State officials have told us that they sometimes must delay work on one report to work on another. For example, State officials told GAO that they delayed work on the report State issued in December 2014 (which covered calendar year 2011) for 4 months so that they could focus on completing delivery of the report to Congress covering calendar year 2010.

As a result of its process, State's delays in reporting on transfers and acquisitions have recently increased. As shown in figure 3, State's report on transfers that first came to its attention in 2010 was provided 26 months after the end of 2010, while its report on transfers that first came to its attention in 2011 was provided 36 months after the end of 2011—a nearly 40 percent increase in the time elapsed between the year addressed and the date that State provided the report. State's draft report on transfers it first learned of in 2012 is now in its 30th month of preparation and, as of April 2015, had fallen 9 months behind the pace set by its predecessor.

Figure 3: State's Delays in Reporting on Transfers and Acquisitions Reportable under the Iran, North Korea, and Syria Nonproliferation Act (INKSNA), 2006–2014



Source: GAO analysis of State data | GAO-15-519

State officials cited two reasons for State's decision to review and report on transfers in groups covering a single year.

- The parties involved in the complex, multistep process can review and clear a single group of transfers per year in sequence more quickly and with less confusion than would be possible with the 6-month cycle required by INKSNA. Officials stated, for example, a shorter cycle could be confusing, as it could require these parties to make decisions on overlapping groups of transfers in different stages of the process in the same time frame.
- While State officials stated they intend to institute 6-month reports once they have cleared the backlog, they acknowledged they might still find it difficult to meet this requirement. INKSNA allows State to add to reportability transfers of items (goods, services, or technologies) not on any of the multilateral control lists that nonetheless make material contributions to WMD. State officials stated that they must complete reports sequentially to ensure that they correctly identify transfers of newly reportable items.

State's Process Limits Its Ability to Minimize the Time Required to Impose INKSNA Sanctions

By using a process that does not comply with INKSA's 6-month reporting cycle, State has limited its ability to minimize delays affecting the potential imposition of INKSNA sanctions. INKSNA does not allow State to impose INKSNA sanctions on foreign persons until State has identified them in a report to the congressional committees. Because State does not have a process enabling it to provide INKSNA reports every 6 months

as required, it cannot impose INKSNA sanctions on foreign persons within the time frames established by INKSNA. Those time frames would allow State to impose sanctions on a foreign person between 6 and 12 months after it first obtained credible information of the person's involvement in a reportable transfer.[11] For example, in any given year in which State decided to sanction a person for a reported transfer or acquisition, the sanction would be effective no later than December if State had learned about the transfer between January 1 and June 30 of that year, if it had identified that person in a report provided to the committees in September as required by INKSNA.

However, State's delay in providing its reports to congressional committees between 2006 and 2014 may undermine its ability to impose potential INKSNA sanctions in accordance within the time frames defined in INKSNA. Because State may not impose INKSNA sanctions on foreign persons until it has identified them in a report, its late reports may have delayed by more than 2 years State's imposition of sanctions on some of these foreign persons. Our analysis of the reports covering the calendar years 2006 through 2011 indicates that State was not able to impose sanctions on foreign persons deemed responsible for transactions included in the reports until an average of 28 months after the end of that reporting period. The intervals ranged between 22 and 36 months.

State's delay in providing its most recent report may have imposed the longest delay on State's ability to impose INKSNA sanctions, which are discretionary. State imposed sanctions on 23 foreign persons in December 2014, when it provided its report on transfers it first learned of in 2011.[12] The sanctions pertained to transfers that had first come to State's attention between 36 and 48 months earlier. If State had established a process enabling it to provide reports to the committees every 6 months, it would have had the ability to impose sanctions on one or more of these 23 persons more than 2 years earlier.

State officials acknowledged these delays, but told us that they believe that the threat of imposing sanctions can be as effective as the imposition of sanctions in achieving the behavior changes that sanctions are intended to motivate. They stated that at various times in the reporting cycle, State may use the information it is compiling to meet the INKSNA reporting requirement to notify foreign governments about suspected transfers taking place within their jurisdictions and request that they take appropriate action. This use is in accordance with provisions in INKSNA that (1) encourage State to contact foreign governments with jurisdiction over the person, in order to afford the government the opportunity to provide explanatory, exculpatory, or additional information with respect to the transfer, and (2) exempt foreign persons from INKSNA sanctions if the foreign government has imposed meaningful penalties on that person. They noted that the threat of INKSNA sanctions itself can prompt foreign governments to

[11] Section 3(b) of INKSNA notes that sanctions on foreign persons will be effective no later than 90 days after the INKSNA report identifying the foreign person is submitted, if the report is submitted on or before the date the reports are due. Therefore, if State provided reports to Congress on March 14 and September 14 every year, as required by INKSNA section 2(b), the Deputy Secretary of State may use his or her discretionary authority to impose sanctions on any or all of the foreign persons named in the reports effective no later than June 14 and December 14, respectively. If reports are submitted to the congressional committees more than 60 days after the required date, any sanctions are effective on the date of the report.

[12] INKSNA sections 4(a) and 4(b) require State to report to the congressional committees when deciding not to exercise the authority to sanction a reportable person, including a written justification describing in detail the facts and circumstances that support the decision not to sanction. 50 U.S.C. § 1701 note.

take actions to halt transfers or to penalize or deter persons within their jurisdiction who are suspected of conducting these transfers, which may stop the activity before it meets the threshold for reporting under INKSNA.

Conclusions

State officials praise INKSNA as a valuable tool in combating proliferation of WMD associated with Iran, Syria, and North Korea. However, State has established a complex and lengthy reporting process that prevents it from providing INKSNA reports on a 6-month schedule to the Senate Committee on Foreign Relations and the House Foreign Affairs Committee, as required by INKSNA. This process may limit State's ability to impose potential sanctions at an earlier date, in accordance with the time frames established in INKSNA.

While State officials state that their process of reviewing and reporting on transfers in groups covering a single calendar year allows them to prepare reports more quickly and with less confusion than groups covering 6 months, our analysis demonstrates that State is falling further and further behind in providing the reports and is now juggling a backlog of draft reports at different stages of that process. In addition, State officials told us that the threat of INKSNA sanctions can be an effective deterrent. However, State's current process has increased the interval of time between the occurrence of a reportable transfer and State's decision to impose sanctions on the foreign persons identified by State as responsible for those transfers. The imposition of sanctions no sooner than 3 or more years after the transfer occurred may diminish the credibility of the threatened sanction. In addition, reporting delays of this magnitude are not consistent with the time frames established by Congress when it enacted INKSNA.

Recommendation for Executive Action

The Secretary of State should reconsider State's INKSNA process to ensure that it (1) complies with INKSNA's 6-month reporting cycle, and (2) minimizes delays in its ability to opt to impose sanctions.

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of State, Commerce, Defense, Energy and Treasury for comment. State provided written comments, which we reprinted in appendix III, as well as technical comments, which we incorporated, as appropriate. Commerce, Defense, Energy, and Treasury declined to provide comments.

In its written comments, State concurred with our recommendation but said they need to clear their backlog before delivering reports semi-annually. Moreover, they expressed concern that the draft report does not take into account the inherent difficulties of meeting the law's very tight deadlines and the substantial increases in scope of reportable activity. In addition, State said that the report does not place sufficient priority on the need for careful preparation and thorough vetting. In response, GAO noted that the report shows that the time State requires to produce the reports for Congress has increased since 2006, the period covered by our report, despite no additional changes to the scope of the law over that period. We also recognize State's need to carefully prepare and thoroughly vet each INKSNA report. We also recognize that some transfers that

are reportable under INKSNA may require several years to investigate and vet prior to being included in an INKSNA report. However, our review found that State's process could allow a single such problematic transfer to delay State's reporting to Congress of other transfers that State may have already investigated and vetted.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, will send copies to the appropriate congressional committees and the Secretaries of State, Commerce, Defense, Energy, and Treasury. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9601 or melitot@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Sincerely yours,

[Signature]

Thomas Melito
Director, International Affairs and Trade

Appendix I
Objectives, Scope, and Methodology

This report (1) examines the Department of State's (State) timeliness in providing Iran, North Korea, and Syria Nonproliferation Act (INKSNA) reports; (2) reviews State's reporting process; and (3) identifies the potential impact of State's reporting timeliness on its imposition of sanctions.

To examine State's timeliness in providing INKSNA reports, we reviewed the reporting requirements established under section 2(b) of INKSNA, the six reports provided by State to the House Committee on Foreign Affairs and the Senate Committee on Foreign Relations covering the period between calendar year 2006—when transfers and acquisitions involving North Korea were first incorporated into the INKSNA reporting requirements—and calendar year 2011, when the latest report was provided by State to the two committees in December 2014. We reviewed the *Federal Register* entries announcing the sanctions on 82 of the foreign persons named in the six reports and the dates those sanctions became effective. We also interviewed officials from the office within State responsible for producing the reports—the Office of Missile, Biological, and Chemical Nonproliferation in the Bureau of International Security and Nonproliferation (ISN/MBC)—the Department of Defense (DOD), and the Department of Energy (Energy) to confirm the timing of these reports.

To review State's reporting process, we reviewed State documents and interviewed officials at State and the Departments of Defense (DOD) and Energy (DOE) to determine the extent to which each agency participated in the State-led interagency working groups that identify transfers potentially meeting INKSNA's reporting and sanctions criteria and their role in the sub-Interagency Policy Committee meetings that voted on which transfers to recommend for reporting and for sanctions. Using the information from these interviews and documents provided by State, we developed a graphic to depict State's process. We requested data from State on the length of time it took to accomplish particular steps in the process for the last six reports and analyzed that data to determine where delays in the process were occurring. We also identified the date that State provided each report and determined the number of months separating that date from the end of the calendar year each report addresses. On the basis of our review, we determined that the data received from the State Department were sufficiently reliable for our analysis of State's process.

In addition, we also interviewed Department of Commerce (Commerce) and Department of the Treasury (Treasury) officials to identify their participation in the INKSNA reporting process.

To identify the potential impact of the timeliness of the INKSNA reports on the imposition of sanctions, we reviewed the deadlines for the imposition of sanctions established in sections 2(b) and 3(c) of INKSNA, the 2006-2011 calendar year INKSNA reports, and the House report that accompanied the bill that became the Iran Nonproliferation Act of 2000. We also interviewed officials from State to discuss the timing and effectiveness of the sanctions.

Appendix II
State's Iran, North Korea, and Syria Nonproliferation Act (INKSNA) Process

According to officials from the Department of State (State) Office of Missile, Biological, and Chemical Nonproliferation in the Bureau of International Security and Nonproliferation (ISN/MBC) State's process for producing the Iran, North Korea, Syria Nonproliferation Act (INKSNA) reports consists of the following steps.

1. Four State-led interagency working groups meet on a regular basis to evaluate reporting from a wide variety of sources on transfers of proliferation concern. The groups also identify activity relevant to INKSNA or other legal authorities.

2. ISN/MBC solicits lists of transfers deemed potentially reportable under INKSNA from the four working groups based on information received during the reporting year. ISN/MBC adds the diplomatic history describing efforts to address transfers with relevant foreign governments, creating a package of information on transfers.

3. ISN/MBC sends the package of transfers to the Intelligence Community for its members to check the information for accuracy and determine whether foreign persons' names are releasable to the *Federal Register* if State decides to impose sanctions on them.

4. ISN/MBC receives a corrected package from the Intelligence Community, sends it out to the federal departments involved in the interagency process (the Departments of Defense, Energy, and Commerce), and the National Security Council (NSC) calls for a sub-Interagency Policy Committee (IPC) meeting to be scheduled to discuss the transfers.

5. Sub-IPC discusses each transaction. Attendees provide advice on whether each transfer is reportable under INKSNA and whether it should result in sanctions.

6. ISN/MBC sends the package of transfers, along with the results of the sub-IPC meeting, to other relevant State regional and functional bureaus to obtain their views and approval.

7. ISN/MBC compiles a draft action memo that contains the recommended outcome for each transfer. The memo also contains the views of the attendees from the sub-IPC meeting. ISN and other relevant management levels clear the memo.

8. ISN sends the action memo to the Office of the Deputy Secretary (D) to review the transfers and the recommended actions and conduct iterative rounds of questions and consultations on certain transfers with other State offices before the memo is ready for the Deputy Secretary of State.

9. The Deputy Secretary of State approves the action memo once he or she makes a decision on every transfer for the given calendar year, and D sends it back to ISN/MBC.

10. ISN/MBC prepares (1) the final INKSNA report for the committees, and (2) the draft *Federal Register* notice. It then sends them to the State Bureau of Legislative Affairs (H).

11. H adds a cover letter and provides the report to the clerks/security officers of recipient committees: the House Committee on Foreign Affairs and the Senate Committee on Foreign Relations.

12. Within days, the *Federal Register* publishes the notice announcing the names of the foreign persons who have been sanctioned.

[Editor's Note: The key to abbreviations from Figure 2 also applies to this Appendix and is reproduced below:

D	Office of the Deputy Secretary of State
Commerce	Department of Commerce
DOD (JCS)	Department of Defense (Joint Chiefs of Staff)
DOD (OSD)	Department of Defense (Office of the Secretary of Defense)
DOE	Department of Energy
H	State Bureau of Legislative Affairs
HFAC	House Committee on Foreign Affairs
IC	Intelligence Community
INKSNA	Iran, North Korea, Syria Nonproliferation Act
ISN	State Bureau of International Security and Nonproliferation
IPC	Interagency Policy Committee
MBC	State Office of Missile, Biological, and Chemical Nonproliferation
NSC	National Security Council
SFRC	Senate Committee on Foreign Relations]

Appendix III
Comments from the Department of State

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



United States Department of State
Comptroller
Washington, DC 20520
MAY 13 2015

Dr. Loren Yager
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "NONPROLIFERATION: State Should Minimize Reporting Delays That may Impact Sanctions on Trade with Iran, North Korea, and Syria" GAO Job Code 321045.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Ralph Palmiero, Deputy Director, Office of Missile, Biological and Chemical Nonproliferation, Bureau of International Security and Nonproliferation at (202) 647-3737.

Sincerely,

Christopher H. Flaggs

Enclosure:
As stated.

cc: GAO – Thomas Melito
ISN – Vann Van Diepen
State/OIG - Norman Brown

Department of State Comments to GAO Draft Report

NONPROLIFERATION: State Should Minimize Reporting Delays That May Impact Sanctions on Trade with Iran, North Korea, and Syria
(GAO-15-519, GAO Code 321045)

The Department appreciates the opportunity to comment on the GAO draft report entitled *"Nonproliferation: State Should Minimize Reporting Delays That may Impact Sanctions on Trade with Iran, North Korea, and Syria."*

General Comments

The draft report regarding the Department's process on the Iran, North Korea, and Syria Nonproliferation Act (INKSNA) does not take into account the inherent difficulties of meeting the law's very tight deadlines and the substantial increases in the scope of reportable activity, pursuant to changes to the original Iran Nonproliferation Act of 2000 (INPA).

See comment 1.

INKSNA continues the original INPA requirement for the reports to identify **every foreign person** determined to be involved in relevant activity based on a deliberately low evidentiary threshold, requiring that we merely possess "credible information indicating that" such activity has occurred, regardless of whether the foreign person "knowingly" engaged in such activity or whether the activity made a "material contribution" to a weapons program. All three of these INPA-now-INKSNA requirements are important factors that expand the scope and complexity of INKSNA reporting and that do not exist in other nonproliferation sanctions legislation.

Further challenging the ability of the Department to deliver INKSNA reports within the statutory timeframe, the law has subsequently expanded in scope along its evolution from INPA to the Iran-Syria Nonproliferation Act (ISNA) to INKSNA, while the above complicating factors (and the statutory deadline) have remained unchanged.

--Initially, the reporting requirement only was for transfers to (not acquisitions from) Iran and did not include the potential for sanctions on most Wassenaar-controlled items. (INKSNA cases involving the transfer or acquisition of Wassenaar-listed items constitute approximately 50% of the current case load.)

--Then, as of January 1, 2005, the law was amended to expand the reporting requirement to include Syria and to require reporting on not only transfers to, but acquisitions from, Iran and Syria. Additionally, a separate requirement was added to report and certify to the Congress to:

- allow payments, in cash or in kind, by the USG to Russia for work to be performed or services to be rendered prior to January 1, 2012 necessary to meet U.S. obligations under agreements related to the International Space Station (ISS); and
- add a reporting requirement on any such payment.

--Finally, as of July 1, 2006, transfers to and acquisitions from North Korea were added to the reporting requirement.

See comment 2.

The draft GAO report also does not place sufficient priority on the need for careful preparation and thorough vetting of a report that must meet the stipulations of U.S. law and has such broad and important implication. The INKSNA sanctions are important tools with implications on bilateral relations, foreign persons/entities, and also U.S. persons' ability to engage with sanctioned entities. The process the Department has established for INKSNA is intended to ensure a full and comprehensive review of potential sanctions actions that have such clear implications. An example of this is the claim that "State has established a complex and lengthy reporting process" on page 18 and elsewhere, implying we could easily make the process less rigorous despite these requirements and implications.

See comment 3.

Given the scope of the INKSNA reporting requirements, the number of cases today is significantly larger than when the only requirement was to report transfers to Iran – although the statutory timelines for sending six-month reports to Congress has not changed. While this does not excuse the current backlog, we believe it is unrealistic to expect such a complex report – involving dozens of sensitive sanctions decisions -- to be turned in every six months within the current statutory timelines. This fact also calls into question the draft report's implicit assumption that a key driver of the current backlog is the Department's ongoing expedient of dealing with that backlog via annual rather than six-monthly reports until the backlog is eliminated. The above factors strongly indicate, however, that had the Department continued trying to submit reports covering six months rather than one year (i.e., combining two reports), that the backlog would have remained – just with twice as many reports backlogged. This likely result is further substantiated by the interdependence of one report on its predecessors in terms of factors like deferred cases and items added to case-by-case reportability.

Department of State Response to Recommendation

The Department of State accepts the GAO recommendation. The Department has every intention of working to comply with INKSNA's 6-month reporting cycle – recognizing the structural impediments noted in the general comments above. We have communicated with the appropriate Congressional committees the need to deliver reports on a calendar year basis at least until the backlog is cleared, and they have made no objections. We then hope to return to the practice of delivering reports semi-annually.

GAO Comment

Comment 1: The scope of INKSNA, as currently written, has not changed since 2006, which was the start time for GAO's analysis. The report shows that the time State requires to produce the reports for Congress has increased since 2006, despite no additional changes to the scope of the law. While INSKNA's six month reporting deadlines may be tight, the report demonstrates that the State Department should consider more efficient processes for meeting those deadlines. For example, State's practice of reporting transfers in entire groups could allow a single problematic transfer to delay the reporting of other transfers that State may have already investigated and vetted.

Comment 2: We recognize State's need to carefully prepare and thoroughly vet each INKSNA report. We also recognize that some transfers that are reportable under INKSNA may require several years to investigate and vet prior to being included in an INKSNA report. However, our review found that State's process could allow a single such problematic transfer to delay State's reporting to Congress of other transfers that State may have already investigated and vetted.

Comment 3: The report highlights the fact that State has opted to submit annual reports instead of the six-month reports required by law. However, it does not assume that State's decision to do so is the key driver of the current backlog. The report instead calls attention to State's current process that could allow a single problematic case in a group to delay its reporting on other transfers within that group. We also note the report demonstrates that the backlog is growing and is not, as State suggests, being eliminated.

Appendix IV
GAO Contact and Staff Acknowledgments

GAO Contact:

Thomas Melito, (202) 512-9601, or melitot@gao.gov

Staff Acknowledgments:

In addition to the contact named above, Pierre Toureille (Assistant Director), B. Patrick Hickey, Jennifer Young, Ashley Alley, Tina Cheng, Debbie Chung, Justin Fisher, and Judy McCloskey made key contributions to this report.

DOCUMENT NO. 10

NORTH KOREA SANCTIONS: UNITED STATES HAS INCREASED FLEXIBILITY TO IMPOSE SANCTIONS, BUT UNITED NATIONS IS IMPEDED BY A LACK OF MEMBER STATE REPORTS

United States Government Accountability Office

Report to the Chairman, Committee on Foreign Relations, U.S. Senate

May 2015

GAO-15-485

GAO Highlights

Highlights of GAO-15-485, a report to the Chairman, Committee on Foreign Relations, U.S. Senate

Why GAO Did This Study

North Korea is a closely controlled society, and its regime has taken actions that threaten the United States and other United Nations member states. North Korean tests of nuclear weapons and ballistic missiles have prompted the United States and the UN to impose sanctions on North Korea.

GAO was asked to review U.S. and UN sanctions on North Korea. This report (1) identifies the activities that are targeted by U.S. and UN sanctions specific to North Korea, (2) describes how the United States implements its sanctions specific to North Korea and examines the challenges it faces in doing so, and (3) describes how the UN implements its sanctions specific to North Korea and examines the challenges it faces in doing so. To answer these questions, GAO analyzed documents from the Departments of State, Treasury, and Commerce, and the UN. GAO also interviewed officials from the Departments of State, Treasury, and Commerce, and the UN.

What GAO Recommends

GAO recommends the Secretary of State work with the UN Security Council to ensure that member states receive technical assistance to help prepare and submit reports on their implementation of UN sanctions on North Korea. The Department of State concurred with this recommendation.

For more information, contact Thomas Melito at (202) 512-9601 or melitot@gao.gov.

What GAO Found

U.S. executive orders (EO) and the Iran, North Korea, and Syria Nonproliferation Act target activities for the imposition of sanctions that include North Korean (Democratic People's Republic of Korea) proliferation of weapons of mass destruction and transferring of luxury goods. The EOs and the act allow the United States to respond by imposing sanctions, such as blocking the assets of persons involved in these activities. United Nations (UN) Security Council resolutions target similar North Korean activities, and under the UN Charter, all 193 UN member states are required to implement sanctions on persons involved in them.

U.S. officials informed GAO that obtaining information on North Korean persons has hindered the U.S. interagency process for imposing sanctions, and that EO 13687, announced in January 2015, provided them with greater flexibility to sanction persons based on their status as government officials rather than evidence of specific conduct. State and Treasury impose sanctions following an interagency process that involves: reviewing intelligence and other information to develop evidence needed to meet standards set by U.S. laws and EOs, vetting possible actions within the U.S. government, determining whether to sanction, and announcing sanctions decisions. Since 2006, the United States has imposed sanctions on 86 North Korean persons, including on 13 North Korean government persons under EO 13687.

Although UN sanctions have a broader reach than U.S. sanctions, the UN lacks reports from many member states describing the steps or measures they have taken to implement specified sanctions provisions. The UN process for imposing sanctions relies on a UN Security Council committee and a UN panel of experts that investigates suspected sanctions violations and recommends actions to the UN. The Panel of Experts investigations have resulted in 32 designations of North Korean or related entities for sanctions since 2006, including a company found to be shipping armaments from Cuba in 2013. While the UN calls upon all member states to submit reports detailing plans for implementing specified sanctions provisions, fewer than half have done so because of a range of factors including a lack of technical capacity. The committee uses the reports to uncover gaps in sanctions implementation and identify member states that require additional outreach. The United States as a member state has submitted all of these

reports. UN and U.S. officials agree that the lack of reports from all member states is an impediment to the UN's implementation of its sanctions.

Abbreviations:

BDA	Banco Delta Asia SARL
Commerce	Department of Commerce
EO	executive order
FinCEN	Financial Crimes Enforcement Network
INPA	Iran Nonproliferation Act of 2000
INKSNA	Iran, North Korea, and Syria Nonproliferation Act
ISNA	Iran and Syria Nonproliferation Ac
North Korea	Democratic People's Republic of Korea
SDN	Specially Designated Nationals
State	Department of State
Treasury	Department of the Treasury
UN	United Nations
UNSCR	UN Security Council Resolution
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USUN	U.S. Mission to the United Nations
WMD	weapons of mass destruction

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

May 13, 2015

The Honorable Bob Corker
Chairman
Committee on Foreign Relations
United States Senate

Dear Mr. Chairman,

In response to North Korea's tests of nuclear weapons and ballistic missiles, beginning in 2006 the United States and the United Nations (UN) have imposed a broad range of sanctions to deter North Korea from proliferating weapons of mass destruction (WMD) and accessing the international financial system.[1] The Department of State (State) and the Department of the Treasury (Treasury) implement and enforce U.S. sanctions, while the Department of Commerce (Commerce) enforces sanctions by limiting the export of U.S. products to North Korea. State is also the lead agency responsible for engagement with the United Nations. The UN Security Council is responsible for ensuring that member states implement and enforce UN sanctions on North Korea. It does so through its 1718 Committee, named after the UN Security Council Resolution (UNSCR) that imposes sanctions on North Korea.[2]

In response to your request, we reviewed U.S. and UN sanctions related to North Korea. This report (1) identifies the activities that are targeted by U.S. and UN sanctions specific to North Korean sanctions, (2) describes how the United States implements its sanctions specific to North Korea and examines the challenges it faces in doing so, and (3) describes how the UN implements its sanctions specific to North Korea and examines the challenges it faces in doing so. This report also includes information comparing U.S. and UN North Korea–specific sanctions with those specific to Iran (see app. I.)

To address our first objective, we reviewed (1) U.S. executive orders (EO) and laws and (2) UNSCRs. We also interviewed officials from State, Treasury, and the UN to confirm the universe of North Korea–specific sanctions. We also interviewed U.S. officials to determine any other executive orders, laws, or resolutions not specific to North Korea that they have used to impose sanctions on North Korea during this time period. We then analyzed the executive orders, laws, and resolutions to identify the activities targeted by the sanctions.

To address our second objective, we interviewed State and Treasury officials to determine the process that each agency follows to impose sanctions on North Korea and related persons.[3] We also interviewed Department of Commerce officials to learn about

[1] The official name of North Korea is the Democratic People's Republic of Korea. For the purposes of this report, we will refer to the country as North Korea.

[2] UN Security Council Resolution 1718 was adopted in October 2006 and imposed a series of economic and commercial sanctions on North Korea. S.C. Res. 1718, U.N. Doc. S/RES/1718 (Oct. 14, 2006).

[3] The term "persons" refers to both individuals and entities. For the purposes of this report, an entity is a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.

how the U.S. government controls exports to North Korea. We also analyzed documents and information from State and Treasury to determine the number of North Korean persons that have been sanctioned since 2006.[4] The challenges discussed herein are based on our discussions with State, Treasury, and Commerce officials. We also reviewed documents such as Federal Register notices and press releases that provided information about U.S. government sanctions to corroborate what officials told us.

To address our third objective, we reviewed UN documents and records of member state implementation reports, and interviewed relevant officials at State, the U.S. Mission to the United Nations, members of the UN 1718 Committee, and former members of the Panel of Experts. To determine the extent to which member states are reporting on their implementation of specified UN sanctions provisions, we examined UN records of member state implementation reports. To identify the challenges the UN faces related to member state reporting and the efforts the UN has taken to help member states report on implementation pursuant to these provisions, we interviewed U.S. officials and Member State delegates to the UN Security Council and representatives on the 1718 Committee, and reviewed UN reports and documents. To examine the efforts the UN has taken to address member state reporting, we interviewed members of the UN 1718 Committee and reviewed documents outlining UN outreach efforts.

To compare U.S. and UN sanctions specific to North Korea and Iran, we reviewed U.S. executive orders and laws and UNSCRs authorizing sanctions that specifically target North Korea and those that specifically target Iran. We analyzed these documents to identify the activities targeted by the sanctions. On the basis of a comprehensive literature review, we developed a list of targeted activities frequently identified in relation to North Korea and Iran sanctions and grouped these activities into high-level categories. To ensure data reliability in categorizing the targeted activities into high-level categories, we conducted a double-blind exercise whereby we individually reviewed the activities identified within the U.S. executive orders and laws and UN resolutions for each country and assigned each activity to a high-level category through consensus. We also had a State Department official review our list of activities and high-level categories to ensure our conclusions were reliable. We then interviewed State and Treasury officials to discuss the differences in activities targeted by North Korea and Iran sanctions. To determine the extent to which member states are reporting on their implementation of specified UN sanctions provisions, we examined the UN 1718 Committee's record of member state implementation reports.[5]

We conducted this performance audit from July 2014 to May 2015 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[4] For a comparison of these sanctions with U.S sanctions on Iran, see app. II.

[5] These reports are formally known as Reports From Member States Pursuant to Paragraph 11 of Resolution 1718 (2006), Paragraph 22 of Resolution 1874 (2009), and Paragraph 25 of Resolution 2094 (2013).

Background

North Korea is an isolated society with a centrally planned economy and a centrally controlled political system. The governing regime assumed power after World War II. Successive generations of a single family have ruled North Korea since its founding. According to the CIA World Factbook, under dictator Kim Jong Un, the grandson of regime founder Kim Il Sung, the regime currently controls all aspects of political life, including the legislative, judicial, and military structures. According to a Library of Congress country study, the North Korean leadership rewards members of the primary political party (the Korean Workers' Party) and the military establishment with housing, food, education, and access to goods. Much of the population, however, lives in poverty, with limited education, travel restrictions, a poor health care system, no open religious institutions or spiritual teaching, and few basic human rights.

North Korea exports commodities such as minerals, metallurgical products, textiles, and agricultural and fishery products. According to the CIA World Factbook, the North Korean economy is one of the world's least open economies. The CIA World Factbook reported that as of 2012, its main export partners were China and South Korea. China is North Korea's closest ally and accounts for almost two-thirds of its trade.

North Korea has engaged in a number of acts that have threatened the security of the United States and other UN member states. Since 2006, North Korea has conducted a number of missile launches and detonated three nuclear explosive devices; torpedoed a South Korean naval vessel, the Cheonan, killing 46 crew members; and launched a disruptive cyberattack against a U.S. company, Sony Pictures Entertainment.[6]

In response to these actions, the United States and the UN imposed sanctions specific to North Korea from 2006 through 2015 (see fig. 1)[7]. The United States has imposed sanctions on North Korea and North Korean persons under EOs and a number of laws and regulations.[8] EOs are issued by the President and generally direct the executive branch to either carry out actions or clarify and further existing laws passed by Congress. Administrations have invoked authority provided by the International Emergency Economic Powers Act, as well as other authorities, to issue EOs specific to North Korea.[9] The UN Security Council issued five UNSCRs imposing sanctions specific to North Korea during this time period.[10] (See fig. 1.)

[6] See the following executive branch press releases regarding these incidents: http://www.treasury.gov/press-center/press-releases/Pages/jl9733.aspx and https://www.whitehouse.gov/the-press-office/statement-press-secretary-republic-korea-navy-ship-cheonan.

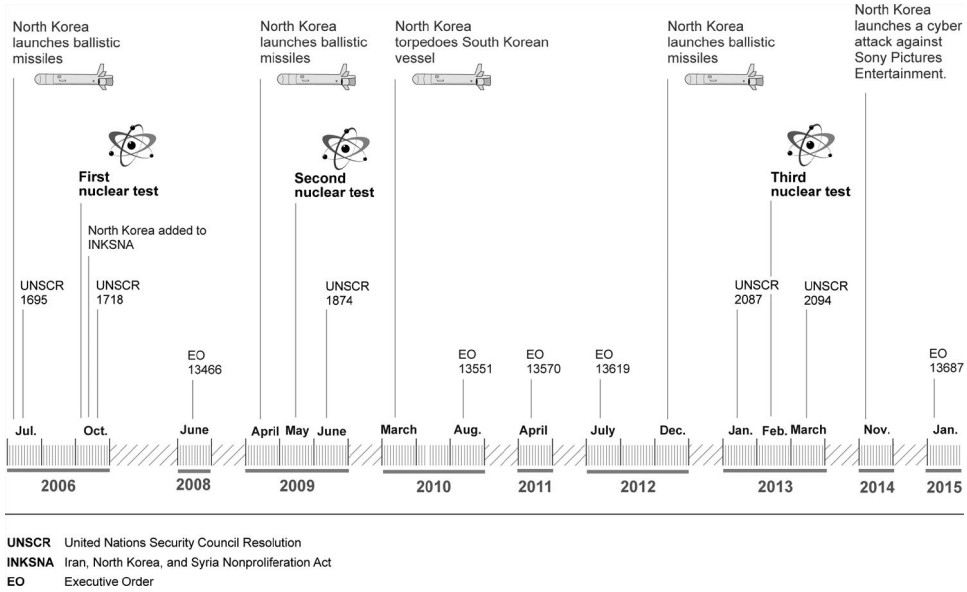
[7] The United States has imposed economic, diplomatic, and political restrictions on North Korea since the outbreak of the Korean War in 1950. This report discusses North Korea—specific sanctions imposed since 2006.

[8] See, e.g., 80 Fed. Reg. 13,667 (Mar. 16, 2015) (Notice of Department of Treasury, Office of Foreign Assets Control: imposition of sanctions pursuant to Executive Order 13687) and 76 Fed. Reg. 30,986 (May 27, 2011) (Notice of Department of State, Bureau of International Security and Nonproliferation: imposition of nonproliferation measures against foreign persons).

[9] 50 U.S.C. §§ 1701–1706. The act granted the President a number of authorities, including the blocking of a foreign country's or foreign national's property, to respond to any unusual and extraordinary threat to the national security, foreign policy, or economy of the United States. See, e.g., Exec. Order No. 13,687, 80 Fed. Reg. 819 (Jan. 2, 2015) and Exec. Order No. 13,570, 76 Fed. Reg. 22,291 (Apr. 18, 2011).

[10] S.C. Res. 1695, U.N. Doc. S/RES/1695 (July 15, 2006); S.C. Res. 1718, U.N. Doc. S/RES/1718 (Oct. 14, 2006); S.C. Res. 1874, U.N. Doc. S/RES/1874 (June 12, 2009); S.C. Res. 2087, U.N. Doc. S/RES/2087 (Jan. 22, 2013);

Figure 1: Timeline of North Korean Actions and United States and United Nations Sanctions



Source: Congressional Research Service, United Nations, The White House, and 50 U.S.C. § 1701 note. | GAO-15-485

U.S. and UN Sanctions Specific to North Korea Target a Range of Activities That Include Proliferation of Weapons of Mass Destruction and Transferring Luxury Goods

U.S. EOs specific to North Korea and the Iran, North Korea, and Syria Nonproliferation Act (INKSNA)[11] authorize the United States to impose sanctions targeting activities that include weapons of mass destruction proliferation, trade in arms and related materiel,[12] and transferring luxury goods.[13] Sanctions that can be imposed pursuant to the EOs and INKSNA include blocking property and banning U.S. government procurement. UNSCRs target similar activities, and under the UN Charter, all 193 UN member states are required to implement sanctions imposed by the UNSCRs, such as travel bans, on North Korean and other persons involved in these activities.

S.C. Res. 2049, U.N. Doc. S/RES/2049 (Mar. 3, 2013). The legal basis for UN sanctions under international law derives from Chapter VII of the UN Charter. Article 41 of Chapter VII addresses enforcement measures not involving the use of armed force and lists examples of specific sanctions measures that the UN may take.

[11] This law was originally enacted as the Iran Nonproliferation Act of 2000 (INPA). The INPA was amended to include Syria in 2005 and became the Iran and Syria Nonproliferation Act, or ISNA. ISNA was amended to include North Korea in 2006, and is now known as the Iran, North Korea, and Syria Nonproliferation Act of 2006 (INKSNA). See Pub. L. No. 106-178, 114 Stat. 38 (codified as amended at 50 U.S.C. § 1701 note).

[12] Exec. Order No. 13,551, 75 Fed. Reg. 53,837 (Aug. 30, 2010).

[13] *Id*.

U.S. Sanctions Target Activities Such as Weapons Proliferation and Trade in Arms

U.S. EOs specific to North Korea and INKSNA authorize the United States to impose sanctions targeting activities that include involvement in North Korean WMD and conventional arms proliferation and transferring luxury goods to North Korea.[14] The most recent EO targets a person's status as opposed to a person's conduct. The EO targets a person's status by authorizing the imposition of sanctions on persons determined, for example, to be agencies, instrumentalities, or controlled entities of the government of North Korea or the Workers' Party of Korea.[15] Table 1 provides examples of the activities and statuses targeted by EOs and INKSNA.[16] In addition, EO 13466 prohibits activities such as the registration of a vessel in North Korea by a U.S. person, and EO 13570 generally prohibits a U.S. person from importing North Korean goods, services, or technology from North Korea.[17]

Table 1: Activities and Statuses Targeted by Sanctions Authorized by U.S. Executive Orders and Law Specific to North Korea

Executive Order (EO) or law and effective date	Examples of targeted activities and statuses
INKSNA (October 13, 2006)[a]	• Transferring to or acquiring from North Korea items listed by multilateral export control regimes, or certain nonlisted items that could materially contribute to weapons of mass destruction (WMD) systems or cruise or ballistic missile systems.
EO 13551 (August 30, 2010)	• Importing, exporting, or reexporting to, into, or from North Korea any arms or related materiel • Providing training, advice, or other services or assistance, or engaging in financial transactions, related to the manufacture, maintenance, or use of any arms or related materiel to be imported, exported, or reexported to, into, or from North Korea • Importing, exporting, or reexporting luxury goods to or into North Korea • Engaging in money laundering, the counterfeiting of goods or currency, bulk cash smuggling, narcotics trafficking, or other illicit economic activity that involves or supports the government of North Korea or any senior official thereof

[14] See, e.g., Pub. L. No. 106-178, as amended; Exec. Order No. 13,619, 77 Fed. Reg. 41,243 (July 11, 2012); and Exec. Order No. 13,551.

[15] Exec. Order No. 13,687.

[16] For a comparison of these sanctions with U.S. sanctions on Iran, see app. II.

[17] Exec. Order No. 13,466, 73 Fed. Reg. 36,787 (June 26, 2008), and Exec. Order No. 13,570, 76 Fed. Reg. 22,291 (Apr. 18, 2011). These EOs are not included in the table because they do not authorize the designations of persons.

Executive Order (EO) or law and effective date	Examples of targeted activities and statuses
	• Providing financial, material, or technological support for, or goods or services to or in support of said activities or persons whose property and interests in property are blocked pursuant to this order • Being owned or controlled by, or acting or purporting to act for or on behalf of, any person whose property and interests in property are blocked pursuant to this order • Attempting to engage in any of said activities
EO 13619 (July 11, 2012)	• Importing, exporting, reexporting, or selling or supplying arms or related materiel from North Korea or the government of North Korea to Burma or the government of Burma • Being a senior official of an entity that engages in above activities in this order • Providing financial, material, or technological support for, or goods and services to or in support of, above activities or persons whose property and interests in property are blocked pursuant to this order • Being owned or controlled by, or acting or purporting to act for or on behalf of, the government of North Korea
EO 13687 (January 2, 2015)	• Being an agency, instrumentality, controlled entity, or official of the government of North Korea or the Workers' Party of Korea • Providing financial, material, or technological support for, or goods or services to or in support of, above activities or persons whose property and interests in property are blocked pursuant to this order • Being owned or controlled by, or acting or purporting to act for or on behalf of, the government of North Korea

Sources: U.S. executive orders and law, and interviews with Department of State and Department of the Treasury officials. | GAO-15-485

[a] Pub. L. No. 106-178 (codified as amended at 50 U.S.C. § 1701 note). INKSNA was originally enacted as the Iran Nonproliferation Act of 2000 in 2000 and was amended to include North Korea on October 13, 2006, by the North Korea Nonproliferation Act of 2006, Pub. L. No. 109-353, 120 Stat. 2015.

Sanctions that can be imposed pursuant to the EOs and law listed above include blocking property and interests in property in the United States, and banning U.S. government procurement and assistance.

The EOs listed in table 1 create a framework within which the executive branch can decide when to impose sanctions against specific persons within the categories established by the EOs, according to Treasury and State officials. Treasury officials informed us that the process of determining whether to impose sanctions on one or more persons is (1) the result of a process wholly under the executive branch, and (2) driven by policy directives that prioritize issues of concern for the agencies. Treasury officials also noted that while Treasury does not consider itself to have discretion on whether or not to

implement an EO, there is discretion at the interagency level regarding what sanctions programs should be focused on for individual designations, and how resources should be allocated among all relevant programs.

INKSNA requires the President to provide reports every 6 months to two congressional committees that identify every foreign person with respect to whom there is credible information indicating that the person, on or after the dates specified in the act, has transferred to, or acquired from, North Korea, Syria, or Iran certain items listed by multilateral export control regimes, or certain nonlisted items that could materially contribute to weapons of mass destruction systems or cruise or ballistic missile systems.[18] It does not require the President to sanction those persons, although it does require him or her to notify the congressional committees if he or she opts not to impose sanctions, including a written justification that supports the President's decision not to exercise this authority.[19] The President has delegated INKSNA authorities to the Secretary of State.[20]

U.S. Agencies Have Used Other Executive Orders and Laws to Target North Korea–Related Activities

In targeting North Korean activities, State and Treasury officials said they have also used EOs and laws that are not specific to North Korea. For example:

- EO 12938[21]—The EO authorizes sanctions on foreign persons that are found to have engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery (including missiles capable of delivering such weapons), including any efforts to manufacture, acquire, possess, develop, transport, transfer, or use such items, by any person or foreign country of proliferation concern.[22] The EO also prohibits the importation of products produced by these persons.[23]
- EO 13382[24]—The EO authorizes the blocking of assets of foreign persons determined by the Secretary of State, in consultation with the Secretary of Treasury, the Attorney General, and other agencies, to have engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of weapons of mass destruction or their means of delivery (including missiles capable of delivering such weapons), including any efforts to manufacture, acquire, possess, develop, transport, transfer,

[18] 50 U.S.C. § 1701 note.

[19] *Id*.

[20] 65 Fed. Reg. 56,209 (Sept. 11, 2000). GAO is currently conducting a separate review of the State Department's implementation of INKSNA, due to be released in May 2015.

[21] Exec. Order No. 12,938, 59 Fed. Reg. 58,099 (Nov. 14, 1994). The current version of section 4 of the executive order, relating to sanctions on foreign persons, was amended by Executive Order 13,094 in 1998 and then by Executive Order 13,382 in 2005. Exec. Order No. 13,094, § 1(a), 63 Fed. Reg. 40,803 (July 28, 1998) and Exec. Order No. 13,382, § 4, 70 Fed. Reg. 38,567 (June 28, 2005).

[22] Exec. Order No. 13,382, § 4 (amending section 4(a) of Executive Order 12,938).

[23] *Id*.

[24] Exec. Order No. 13,382.

or use such items, by any person or foreign country of proliferation concern.[25] EO 13382 also authorizes Treasury to impose sanctions after Treasury determines, in consultation with State and other relevant agencies, that a person has provided, or attempted to provide, financial, material, technological, or other support for such activities to persons whose assets are blocked under this EO.[26]

- Missile Sanctions Law[27]—These laws generally provide for mandatory sanctions against any foreign person determined to have knowingly exported, transferred, or otherwise engaged in trade, after November 1990, of Missile Technology Control Regime Annex items that contribute to the acquisition, design, development, or production of certain missiles in a country that is not a signatory to the Missile Technology Control Regime. Sanctionable activity under the Missile Sanctions laws includes exporting, transferring, or otherwise engaging in the trade of any Missile Technology Control Regime equipment or technology that contributes to the acquisition, design, development, or production of missiles in a country that is not a Missile Trade Control Regime adherent.
- The USA PATRIOT Act[28]—Section 311 of the USA PATRIOT Act is a U.S. tool implemented by Treasury's Financial Crimes Enforcement Network (FinCEN) to address the threat to the U.S. financial system of money laundering and terrorist financing. Section 311 grants the Secretary of the Treasury the authority, upon finding that reasonable grounds exist for concluding that a foreign jurisdiction, foreign financial institution, class of transaction, or type of account is of primary money laundering concern, to require domestic financial institutions to take certain special measures upon making the finding of primary money laundering concern. This authority provides the Treasury with a range of options that can be adapted to protect the U.S. financial system from specific money laundering and terrorist financing risks. The Secretary of the Treasury has delegated implementation of Section 311 to the Director of FinCEN. In 2007, FinCEN issued a final rule pursuant to section 311 that prohibited covered financial institutions from opening or maintaining correspondent accounts in the United States for, or on behalf of, a Macao bank (Banco Delta Asia SARL).[29] FinCEN cited the bank's facilita-

[25] Exec. Order No. 13,382, § 1(a)(ii).

[26] Exec. Order No. 13,382, § 1(a)(iii).

[27] State refers to section 73 of the Arms Export Control Act and section 11B of the Export Administration Act collectively as the Missile Sanctions laws. See 22 U.S.C. § 2797b and 50 U.S.C. App. § 2410b.

[28] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001) (codified at 31 U.S.C. § 5318A). For more information on section 311 of the USA PATRIOT Act, see GAO, *USA PATRIOT Act: Better Interagency Coordination and Implementing Guidance for Section 311 Could Improve U.S. Anti-Money Laundering Efforts*, GAO-08-1058 (Washington, D.C.: Sept. 30, 2008).

[29] 72 Fed. Reg. 12,730 (Mar. 19, 2007). In 2013, Banco Delta Asia SARL (BDA) and its parent company, Delta Asia Group Ltd., filed a civil complaint in U.S. District Court against FinCEN, its director, as well the U.S. Secretary of the Treasury in their respective official capacities, seeking, among other things, review under the Administrative Procedure Act of FinCEN's final rule imposing a special measure against BDA, pursuant section 311 of the USA PATRIOT Act (31 U.S.C. § 5318A). *Banco Delta Asia, S.A.R.L. v. Fin. Crimes Enforcement Network,* No. 1:13-cv-00333-BAH (D.D.C.). In November 2010, BDA separately filed an administrative petition with FinCEN to repeal the rule. Parties began discussions to address the administrative petition, and in February 2014, the parties jointly requested a stay in the lawsuit in anticipation that their discussions may resolve the litigation. The court granted the motion for a stay in the case, and the stay has been extended to February 29, 2016. This report does not express any opinion regarding the BDA litigation.

tion of financial transactions conducted by North Korean– related accounts that related to money laundering and illicit activities, including trade in counterfeit U.S. currency, counterfeit cigarettes, and narcotics, as grounds for its action.

UN Sanctions Target Activities Such as Weapons Proliferation and Financial Transactions

Five UNSCRs target North Korean–related activities that include WMD proliferation, cash transfers, and trade in luxury goods to North Korea (see table 2). Under the UN Charter, all 193 UN member states are required to implement sanctions in the UNSCRs that include imposing an arms embargo, prohibiting travel, and freezing assets. State officials told us that UN sanctions can amplify U.S. development of bilateral sanctions specific to North Korea, and that the United States has imposed sanctions beyond those required by UNSCRs. According to State officials, the United States has implemented the sanctions within the UNSCRs, pursuant to authorities including the United Nations Participation Act of 1945.[30]

Table 2: Targeted Activities within United Nations Security Council Resolutions Imposing Sanctions Specific to North Korea

United Nations Security Council resolution (UNSCR) and date	Examples of targeted activities
UNSCR 1695 (July 15, 2006)	• Transferring missiles and missile-related items, materials, goods, and technology to North Korea's missile or weapons of mass destruction (WMD) programs • Procuring missiles or missile-related-items, materials, goods, and technology from North Korea and transferring any financial resources in relation to North Korea's missile or WMD programs
UNSCR 1718 (October 14, 2006)	• Supplying, selling, or transferring to North Korea any battle tanks, armored combat vehicles, large-caliber artillery systems, combat aircraft, attack helicopters, warships, missiles, or missile systems as defined for the purpose of the United Nations Register on Conventional Arms, or related materiel including spare parts • Supplying, selling, or transferring luxury goods to North Korea • Procuring from North Korea items that, as determined by the Security Council or the 1718 Committee, could contribute to nuclear-related, ballistic missile–related, or other weapons of mass destruction–related program • Transferring to or from North Korea technical training, advice, services, or assistance related to the provision, manufacture, maintenance, or use of specified items related to WMD

[30] Ch. 583, 59 Stat. 619 (1945).

United Nations Security Council resolution (UNSCR) and date	Examples of targeted activities
	• Allowing the entry into or transit through states' territories of persons designated as being responsible for, including through supporting or promoting, North Korean policies in relation to North Korea's nuclear-related, ballistic missile—related, and other weapons of mass destruction—related programs, together with their family members
UNSCR 1874 (June 12, 2009)	• Entering into new commitments for grants, financial assistance, or concessional loans to North Korea • Providing public financial support for trade with North Korea (including the granting of export credits, guarantees, or insurance to their nationals or entities involved in such trade) where such financial support could contribute to North Korea's nuclear-related or ballistic missile—related or other WMD-related programs or activities
UNSCR 2087 (January 22, 2013)	• Activities of nationals, persons in states' territories, financial institutions, and other entities organized under states' laws (including branches abroad) that are with or on behalf of financial institutions in North Korea, or of those that act on behalf or at the direction of North Korean financial institutions, including their branches, representatives, agents, and subsidiaries abroad • The entry into or transit through states' territories of individuals working on behalf or at the direction of a designated individual or entity
UNSCR 2094 (March 7, 2013)	• The entry into or transit through member states' territories of individuals acting on behalf or at the direction of persons designated by the United Nations (UN) • Certain brokering or other intermediary services, including when arranging for the provision, maintenance, or use of prohibited items in other states or the supply, sale, or transfer to or exports from other states • The opening of new branches, subsidiaries, or representative offices of North Korean banks; North Korean banks establishing new joint ventures and taking an ownership interest in or establishing or maintaining correspondent relationships with banks in their jurisdiction; the provision of financial services for activities that could contribute to North Korea's nuclear or ballistic missile programs, or other prohibited activities • Transfers to North Korea of bulk cash, including through cash couriers, transiting to and from North Korea

Sources: United Nations Security Council resolutions and interviews with Department of State officials. | GAO 15-485

Recent EO Can Help Address Factor Hindering U.S. Process for Imposing Sanctions Related to North Korea

U.S. officials informed GAO that obtaining information on North Korean persons has hindered the U.S. interagency process for imposing sanctions, and that a recent EO has provided them with greater flexibility to sanction persons based on their status as government or party officials rather than evidence of specific conduct. EO 13687 allows State and Treasury to sanction persons because they are officials of the North Korean government or of the Worker's Party of Korea, instead of based on specific conduct. State and Treasury impose sanctions following an interagency process that involves reviewing intelligence and other information to develop evidence needed to meet standards set by U.S. laws and EOs, vetting possible actions within the U.S. government, determining whether and when to sanction, and announcing sanctions decisions. Since 2006, the United States has imposed sanctions on 86 North Korean persons, including 13 North Korean government officials and entities, under EO 13687. Commerce is the U.S. government agency that controls exports by issuing licenses for shipping goods that are not prohibited to North Korea.

A Lack of Information about North Korean Persons Hinders the Sanctions Determination Process

Agency officials cited obtaining sufficient information about North Korean persons to be their greatest challenge in making sanctions determinations. Most North Korea–specific sanctions authorities require a determination that a person engaged in a specific activity.[31] Officials said that for sanctions to be effective, financial institutions need a minimum set of identifying information so that they can ensure they are blocking the right person. However, officials said that gathering information on the activities of North Korean persons and personal identifying information can be difficult because of the nature of North Korean society, whose citizens are tightly controlled by the government. Without sufficient information, the United States could mistakenly designate and therefore block the assets of the wrong person, particularly one with a common surname. State officials also cited obtaining sufficient information as a challenge to North Korean sanctions implementation, especially if the sanctions authority requires information indicating that the foreign person knowingly engaged in sanctionable activities. Officials in both agencies also said that they face challenges in obtaining information that can be made public in the Federal Register.

New Executive Order Provides State and Treasury Greater Flexibility and Can Address Factors Hindering U.S. Sanctioning Process

State and Treasury officials informed us that EO 13687, issued on January 2, 2015, gives them greater flexibility to impose sanctions despite the lack of complete information

[31] See, e.g., Exec. Order No. 13,551 (authorizing the imposition of sanctions if Treasury determines that a person "directly or indirectly, imported, exported, or reexported to, into, or from North Korea any arms or related materiel").

about persons' activities. Treasury officials noted that sanctions under EO 13687 are status-based rather than conduct-based, which means that the EO allows agencies to sanction persons, for example, based on their status as North Korean government officials, rather than on their engagement in specific activities. EO 13687 allows Treasury to designate persons based solely on their status as officials, agencies, or controlled entities of the North Korean government, and to designate other persons acting on their behalf or providing them with material support.[32] According to Treasury, EO 13687 represents a significant broadening of Treasury's authority to increase financial pressure on the North Korean government and to further isolate North Korea from the international financial system. The White House issued the EO in response to North Korean cyberattacks on Sony Pictures Entertainment in November and December 2014. Treasury officials also noted that although the new authority allows them to target any North Korean government official, they continue to target activities prohibited under current sanctions, such as WMD proliferation.

Sony Cyberattacks

On November 24, 2014, Sony Pictures Entertainment experienced a cyberattack that disabled its information technology, destroyed data, and released internal e-mails. Sony also received e-mails threatening terrorist attacks on theaters scheduled to show a film, *The Interview,* which depicted the assassination of Kim Jong Un. The Federal Bureau of Investigation and the Director of National Intelligence attributed these cyberattacks to the North Korean government.

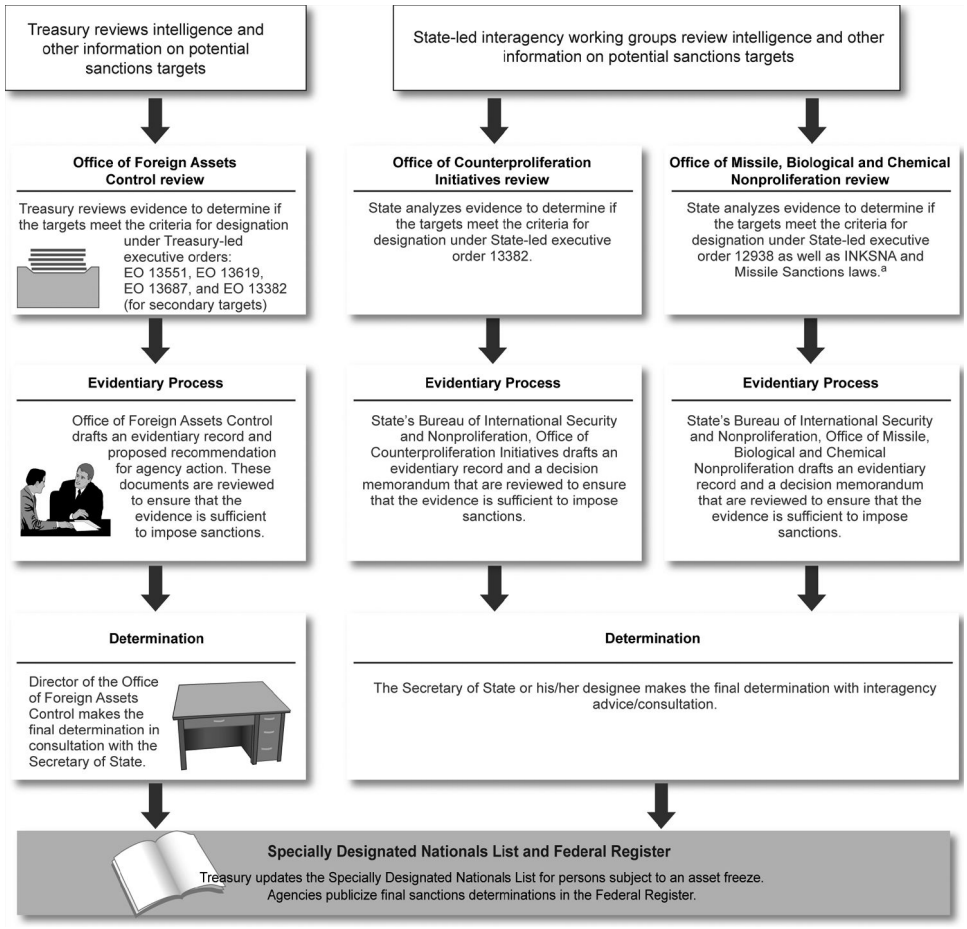
Source: Congressional Research Service. | GAO-15-485

U.S. Agencies Use an Interagency Process to Determine When and Whether to Impose Sanctions

Treasury and State officials informed us that they have established processes to determine when and if the United States should impose sanctions related to North Korea. The processes involve reviewing evidence to identify sanctions targets, ensuring that they have adequate evidence to sanction, and imposing and publicizing the sanctions. (See fig. 2.)

[32] Exec. Order No. 13,687, § 1.

Figure 2: U.S. Process for North Korea Sanctions Determinations



Source: GAO analysis based on interviews with officials from the Departments of State and Treasury. | GAO-15-485

[a] Iran, North Korea, and Syria Nonproliferation Act, codified at 50 U.S.C. § 1701 note.

Treasury Officials and State-Led Working Groups Review Intelligence and Other Information on Potential Targets

For North Korea-specific sanctions that fall under Treasury's jurisdiction, Treasury officials said they investigate and collaborate with other U.S. government agencies to identify specific targets. The Office of Foreign Assets Control investigates the target's activities and communicates with Treasury and other agency officials about the potential target. Where appropriate, Treasury will notify foreign authorities of the activities of the targeted person and seek commitment to stop the activity.

State-Led Working Groups

- *Nuclear Interdiction Action Group*
- *SHIELD Chemical and Biological Weapons Group*
- *Technology Transfer Working Group*
- *Missile Trade Analysis Group*

Source: GAO analysis based on State Department data. | GAO-15-485

State's Bureau of International Security and Nonproliferation's Office of Counterproliferation Initiatives leads an interagency process to evaluate whether a person's activities are potentially sanctionable under EO 13382, which targets proliferation of weapons of mass destruction. The Office of Missile, Biological and Chemical Nonproliferation, also under the Bureau of International Security and Nonproliferation, leads the process for INKSNA, EO 12938, and the Missile Sanctions laws. The process begins with four State-led interagency working groups responsible for coordinating nonproliferation efforts involving (1) chemical and biological weapons, (2) missile technology, (3) nuclear technology, and (4) advanced conventional weapons. Each working group is chaired by a State official and consists of representatives from several U.S. government departments and agencies such as the Departments of Defense, Commerce, Homeland Security, Treasury, and Energy; the Federal Bureau of Investigation; and various intelligence community agencies. State officials said that the working groups regularly evaluate reports concerning proliferation-related activities and determine an appropriate response to impede activities of concern. As part of this review process, these groups identify transactions that may be sanctionable under various nonproliferation sanction authorities, including those related to North Korea. According to State and other working group officials, the interagency review process relies on criteria defined in the laws and EOs when assessing a transaction for the potential application of those sanctions. State officials also said the groups do not pursue sanctions for a target if they determine available information does not provide a basis for applying sanctions or is not legally sufficient.

State and Treasury Seek Consensus before Making a Final Determination

Officials in each agency said that they follow an evidence-based process to gain inter- and intra-agency consensus on imposing sanctions.

- At Treasury, Office of Foreign Assets Control officials said that they create an evidentiary record that contains the information they have gathered on a targeted person to present sufficient evidence that the person has engaged in sanctionable activity. The record contains identifying information such as date of birth, place of birth, or passport information, or if the targeted person is a company, the identifying information might be an address or telephone number. After the Office of Foreign Assets Control has approved this document, it is further reviewed for legal sufficiency by the Department of Justice, Department of State, and other relevant agencies.

- At State, the Offices of Counterproliferation Initiatives and Missile, Biological and Chemical Nonproliferation draft a statement of facts that provides a summary of intelligence available on a targeted transaction. Concurrently, State drafts a policy memo that explains the legal justification for the case. State circulates these documents internally and obtains advice from appropriate agencies and, in the case of actions targeted under EO 13382, consults with Treasury's Office of Foreign Assets Control. Officials from the Offices of Counterproliferation Initiatives and Missile, Biological and Chemical Nonproliferation also said they circulate a decision memorandum to relevant stakeholders for approval.

Officials at State and Treasury also told us that their process includes steps for making and announcing final sanctions determinations.

- At Treasury, the Office of Foreign Assets Control makes the final determination. Officials then publicize the sanctions in the Federal Register.
- At State, once the stakeholders have cleared the memorandum, the Offices of Counterproliferation Initiatives and Missile, Biological and Chemical Nonproliferation forward it to the Secretary of State or his or her designee for a final sanctions determination. They then prepare a report on imposed sanctions for publication in the Federal Register.

When State or Treasury makes a determination that results in blocked assets, Treasury places the sanctioned person on the Specially Designated Nationals and Blocked Persons (SDN) list indicating that the person's assets are blocked. Pursuant to regulation, U.S. persons, including banks, are required to block any assets of such persons that are in their possession or that come within their possession.[33] As a consequence of the blocking, U.S. persons are generally prohibited from engaging in activities with the property or interests in property of persons on the SDN list.[34] U.S. citizens are generally prohibited from doing business with individuals and persons on the SDN list.[35] Treasury officials noted that persons' status on this list does not expire, but persons may apply to be taken off the list. However, no North Korean person has asked for his or her name to be removed.

State and Treasury Have Sanctioned 86 North Korean Persons since 2006

Since 2006, the United States has imposed sanctions on 86 North Korean persons under five EOs, INKSNA, and Missile Sanctions laws (see table 3). The most frequently used EO during this time period was EO 13382, which, as noted above, is not specific to North Korea. Treasury imposed the most recent sanctions on North Korean persons in January 2015, in response to North Korea's cyberattacks on Sony Pictures. In response, Treasury placed 10 North Korean individuals on the SDN list, and updated information about 3 persons on the list.

[33] 31 C.F.R. part 510.

[34] 31 C.F.R. part 510.

[35] Please see Treasury's website: http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx for the complete list of Specially Designated Nationals.

Table 3: State and Treasury Have Sanctioned 86 North Korean Persons, Calendar Years 2006–2015

Executive order/law	Number of North Korean persons sanctioned
EO 13382	43
EO 13687	13
EO 13551	9
INKSNA[a]	8
EO 13619	5
EO 12938	4
Missile Sanctions laws (Arms Export Control Act and Export Administration Act)[b]	4
Total	**86**

Sources: GAO analysis of Treasury and State data. | GAO-15-485

[a] Iran, North Korea, and Syria Nonproliferation Act , codified at 50 U.S.C. § 1701 note.

[b] 22 U.S.C. § 2797b and 50 U.S.C. App. § 2410b.

State and Treasury have used EO 13382 most frequently—43 times in 10 years—to impose sanctions on North Korean persons that they found had engaged in activities related to WMD proliferation. For example, in March 2013, Treasury used EO 13382 to designate the following for sanctions:

- North Korea's primary foreign exchange bank, which facilitated millions of dollars in transactions that benefited North Korean arms dealing.
- The chairman of the North Korean committee that oversees the production of North Korea's ballistic missiles.
- Three North Korean government officials who were connected with North Korea's nuclear and ballistic weapons production. According to the Federal Register notice, the United States imposed sanctions on these persons because State determined that they "engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of WMD or their means of delivery (including missiles capable of delivering such weapons), including any efforts to manufacture, acquire, possess, develop, transport, transfer or use such items, by any person or foreign country of proliferation concern."[36]

Commerce Enforces Export Controls On Items That Are Shipped to North Korea

Commerce's Bureau of Industry and Security requires those exporters who wish to ship items to North Korea to obtain a license for dual-use items that are subject to the

[36] 78 Fed. Reg. 17,996 (Mar. 25, 2013).

Export Administration Regulations.[37] Dual-use items are goods and technology that are designed for commercial use but could have military applications, such as computers and telecommunications equipment. In general, the Bureau of Industry and Security reviews applications for items requiring a license for export or reexport to North Korea and approves or denies applications on a case-by-case basis. According to the Bureau of Industry and Security, it will deny a license for luxury goods or any item that could contribute to North Korea's nuclear-related, ballistic missile–related, or other WMD-related programs. Commerce officials informed us that they receive relatively few requests for licenses to export items to North Korea and in most of these cases Commerce issues a license because most of the applications are for humanitarian purposes. In 2014, the Bureau of Industry and Security approved licenses for items such as telecommunications equipment and medical devices, as well as water well–drilling equipment and volcanic seismic measuring instruments.

Commerce does not require a license to export some items, such as food and medicine, to North Korea.[38] Commerce officials informed us that, under the Export Administration Regulations, the Bureau of Industry and Security, in consultation with the Departments of Defense and State, will generally approve applications to export or reexport humanitarian items, such as blankets, basic footwear, and other items meeting subsistence needs that are intended for the benefit of the North Korean people. For example, it will approve items in support of UN humanitarian efforts, and agricultural commodities or medical devices that the Bureau of Industry and Security determines are not luxury goods.

The UN Implements Sanctions on North Korea but Lacks Implementation Reports from More than Half of Member States

While UN sanctions have a broader reach than U.S. sanctions because all UN member states are obligated to implement and enforce them, the UN does not know the extent to which members are actually implementing its sanctions. The UN process for imposing sanctions on North Korea or related persons relies on a Security Council committee and a UN panel of experts that investigates suspected violations of North Korea sanctions and recommends actions to the UN. The panel has found North Korean persons using illicit techniques to evade sanctions and trade in arms and related material and has designated 32 North Korean or related entities for sanctioning since 2006, including a North Korean company found to be shipping armaments from Cuba to North Korea. However, while the UN calls upon member states to submit reports describing the steps or measures they have taken to implement effectively specified sanctions provisions, fewer than half have done so. According to UN and U.S. officials, many member states lack the technical capacity to develop the reports and implement sanctions. Member state delegates to the UN Security Council and U.S. officials agree that the lack of reports from all member states is an impediment to UN sanctions implementation.

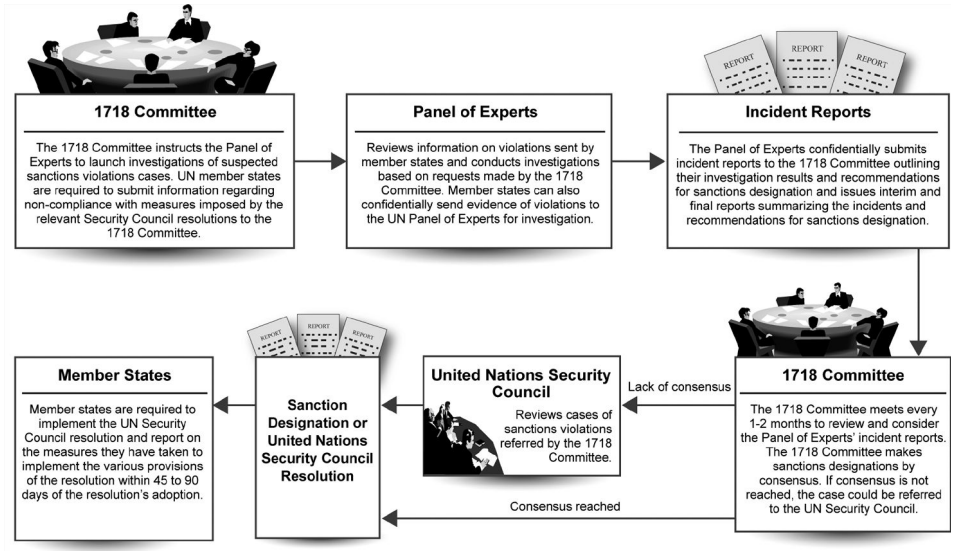
[37] 15 C.F.R. §§ 746.1, 746.4.

[38] 15 C.F.R. § 746.4(a).

The 1718 Committee Oversees North Korea Sanctions

Member state delegates to the UN Security Council informed us that the UN has established a process to determine when and if to impose sanctions on persons that have violated the provisions of UNSCRs. The process involves the Security Council committee established pursuant to Security Council Resolution 1718 that oversees UN sanctions on North Korea; the Panel of Experts, which reviews information on violations of North Korea sanctions sent by member states and conducts investigations based on requests from the committee; and member states whose role is to implement sanctions on North Korea as required by various UN Security Council resolutions. (See fig. 3.)

Figure 3: United Nations North Korea Sanctions Designation Process



Source: GAO analysis of UN data. | GAO-15-485

The UN established the committee in 2006.[39] It consists of 15 members, including the 5 permanent members of the United Nations Security Council and 10 nonpermanent members.[40] The committee makes all decisions by consensus and is mandated to seek information from member states regarding their actions to implement the measures imposed by UNSCR 1718.[41] It is also mandated to examine and take action on information regarding alleged sanctions violations, consider and decide upon requests for

[39] S.C. Res. 1718, para. 12, U.N. Doc. S/RES/1718 (Oct. 14, 2006).

[40] The 5 permanent members of the United Nations Security Council are China, France, Russia, the United Kingdom, and the United States. The current 10 nonpermanent members of the United Nations Security Council are Angola, Chad, Chile, Jordan, Lithuania, Malaysia, New Zealand, Nigeria, Spain, and Venezuela.

[41] As noted previously, UN Security Council Resolution 1718 was adopted in October 2006 and imposes a series of economic and commercial sanctions on North Korea. S.C. Res. 1718, para. 12, U.N. Doc. S/RES/1718 (Oct. 14, 2006) (establishing the mandate of the committee).

exemptions, determine additional items to be added to the list of sanctioned goods, designate individuals and entities for sanctions, promulgate guidelines to facilitate the implementation of sanctions measures, and report at least every 90 days to the UN Security Council on its work overseeing sanctions measures set out in United Nations Security Council resolution 1718 on North Korea.[42]

The Panel of Experts Monitors and Facilitates Implementation of United Nations Sanctions on North Korea

The Panel of Experts was established in 2009 as a technical body within the committee. Pursuant to UNSCR 1874, the panel is tasked with, among other things, gathering, examining, and analyzing information regarding incidents of noncompliance with United Nations Security Council sanctions on North Korea.[43] The panel was originally created for a 1-year period, but the Security Council extended the panel's mandate in subsequent resolutions.[44] The panel acts under the committee's direction to implement its mandate to gather, examine, and analyze information from member states, relevant UN bodies, and other interested parties regarding North Korea sanctions implementation. The panel does not have enforcement authority and relies on the cooperation of member states to provide information that helps it with its investigations.

The panel consists of eight subject matter experts from UN member states, including representatives from the council's 5 permanent members. The Secretary General appoints panel members, who currently are from China, France, Japan, Russia, South Africa, South Korea, the United Kingdom, and the United States. According to the UN, these subject matter experts specialize in technical areas such as WMD arms control and nonproliferation policy, customs and export controls, finance, missile technology, maritime transport, and nuclear issues. According to a representative of the committee, panel members are not intended to represent their countries, but to be independent in order to provide objective assessments.

According to UN guidance, the panel reviews public information and conducts investigative work on incidents or events, and consults foreign governments and seeks information beyond what member states provide them. Representatives of the U.S. Mission to the United Nations (USUN) informed us that the United States and other countries provide the panel with information to help facilitate investigations. The UN Security Council encourages UN member states to respond promptly and thoroughly to the panel's requests for information and to invite panel members to visit and investigate alleged violations of the sanctions regime, including inspection of items that might have been seized by national authorities.

[42] S.C. Res. 1718, para. 12, U.N. Doc. S/RES/1718 (Oct. 14, 2006) (establishing the mandate of the committee). United Nations Security Council resolutions on North Korea include UNSCR 1695, UNSCR 1718, UNSCR 1874, UNSCR 2087, and UNSCR 2094. See S.C. Res. 1695, U.N. Doc. S/RES/1695 (July 15, 2006); S.C. Res. 1718, U.N. Doc. S/RES/1718 (Oct. 14, 2006); S.C. Res. 1874, U.N. Doc. S/RES/1874 (June 12, 2009); S.C. Res. 2087, U.N. Doc. S/RES/2087 (Jan. 22, 2013); and S.C. Res. 2049, U.N. Doc. S/RES/2049 (Mar. 3, 2013).

[43] S.C. Res. 1874, para. 26, U.N. Doc. S/RES/1874 (June 12, 2009). As noted previously, the UN adopted UNSCR 1874 in June 2009. Although the original mandate of the panel referred only to provisions in UNSCR 1718 and 1874, the panel's mandate has been expanded to cover later resolutions.

[44] S.C. Res. 1874, para. 26, U.N. Doc. S/RES/1874 (June 12, 2009). UNSCR 2094 extended the Panel of Experts' mandate, which has been expanded to cover the new measures imposed by that resolution.

Following investigations of suspected sanctions violations, the panel submits investigative reports (incident reports) to the committee detailing its findings and recommendations on how to proceed, according to UN guidance. The panel treats its incident reports as confidential and provides access only to committee and Security Council members. According to a representative of the committee, the committee considers the violations and recommendations and makes sanctions designations based on the consensus of committee members. According to a representative of the committee, if the committee does not reach consensus, it can refer the case to the UN Security Council, pending member agreement.

Ultimately, the UN Security Council determines whether or not recommended designations meet the criteria for sanctions, according to a representative of the committee. If the decision is affirmative, it takes action by making sanctions designations mostly through new resolutions. This process has resulted in 32 designations since 2006. All but one of these designations were made through new resolutions, according to a USUN official. For example, the committee designated the Ocean Maritime Management Company for sanctions through the committee process in July 2014. The panel is generally required, with each extension of its mandate, to provide the committee with an interim and final report, including findings and recommendations.[45]

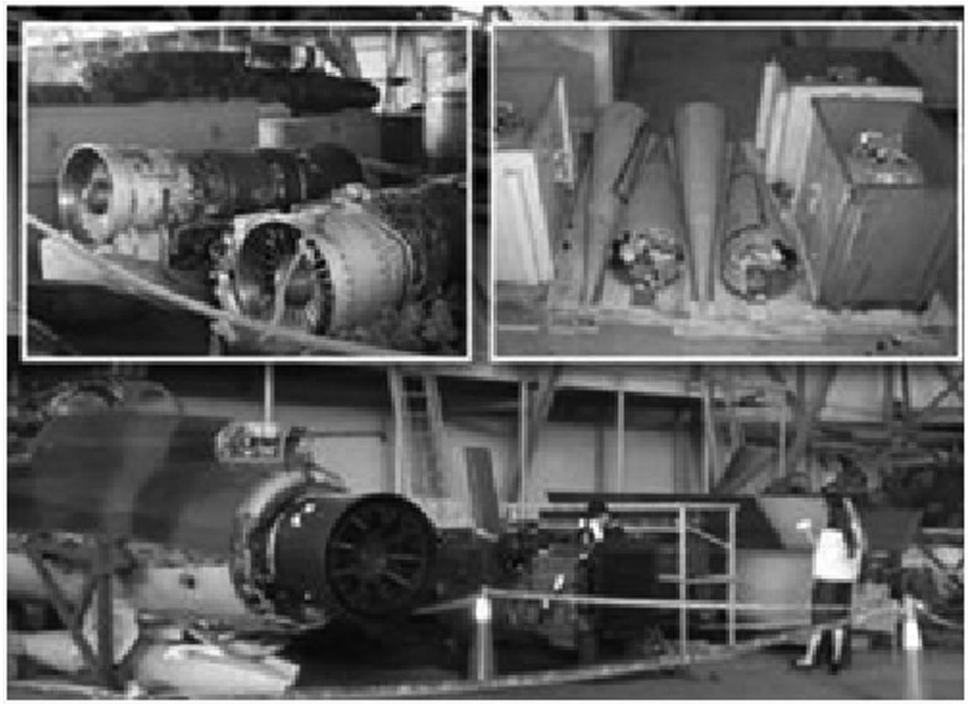
North Korea Uses Illicit Techniques to Evade Sanctions and Trade in Arms and Related Material

The panel's final reports have identified North Korea's use of evasive techniques to export weapons. The panel's 2014 final report described North Korea's attempt to illicitly transport arms and related materiel from Cuba to North Korea concealed underneath thousands of bags of sugar onboard the North Korean vessel Chong Chon Gang.[46] North Korea's use of evasive techniques in this case was blocked by actions taken by Panama, a UN member state. Panamanian authorities stopped and examined the Chong Chon Gang vessel as it passed through Panama's jurisdiction. After uncovering items on the vessel that it believed to be arms and related materiel, Panama alerted the committee of the possible UN sanctions violation. According to representatives of the committee, Panama cooperated with the panel as it conducted its investigation. The panel concluded that the shipment was in violation of UN sanctions and that it constituted the largest amount of arms and related materiel interdicted to North Korea since the adoption of UNSCR 1718. The committee placed the shipping company that operated the Chong Chon Gang on its sanctioned entities list.

[45] The panel was established pursuant to UNSCR 1874. S.C. Res. 1874, para. 26, U.N. Doc. S/RES/1874 (June 12, 2009). Its mandate has been extended by UNSCR 1928, UNSCR 1985, UNSCR 2050, UNSCR 2094, UNSCR 2141, and UNSCR 2207. S.C. Res. 2207, para. 1-2, U.N. Doc. S/Res/2207 (Mar. 4, 2015); S.C. Res. 2141, para. 1-2, U.N. Doc. S/Res/2141 (Mar. 4, 2014); S.C. Res. 2094, para. 29, U.N. Doc. S/Res/2094 (Mar. 7, 2013); S.C. Res. 2050, para. 1-2, U.N. Doc. S/Res/2050 (June 12, 2012); S.C. Res. 1985, para. 1-2, U.N. Doc. S/Res/1985 (June 10, 2011); and S.C. Res. 1928, para. 1-2, U.N. Doc. S/Res/1928 (June 7, 2010). Panel of Experts reports can be found on the committee's website, at http://www.un.org/sc/committees/1718/poereports.shtml. The consolidated list of designated entities and individuals can be found on the committee's website, at http://www.un.org/sc/committees/1718/sanctions_list.shtml.

[46] The Panel of Experts' 2014 final report containing a summary of the *Chong Chon Gang* case can be found on the committee's website, at http://www.un.org/ga/search/view_doc.asp?symbol=S/2014/920.

Figure 4: Shipment of Arms Found Concealed on North Korean Vessel Chong Chon Gang



Source: United Nations. | GAO 15-485

The panel's investigations have also uncovered evidence of North Korea's efforts to evade sanctions by routing financial transactions in support of North Korea's procurement of sanctioned goods through intermediaries, including those in China, Malaysia, Singapore, and Thailand. For instance, in its investigation of the Chong Chon Gang case, the panel found that the vessel operator, North Korea's Ocean Maritime Management Company, Limited, used foreign intermediaries in Hong Kong, Thailand, and Singapore to conduct financial transactions on its behalf. The panel also identified that in most cases the investigated transactions were made in United States dollars from foreign-based banks and transferred through corresponding bank accounts in the United States. The panel's 2015 final report indicated that North Korea has successfully bypassed banking organizations' due diligence processes by initiating transactions through other entities on its behalf. The panel expressed concern in its report regarding the ability of banks in countries with less effective banking regulations or compliance institutions to detect and prevent illicit transfers involving North Korea.

More than Half of All UN Member States Have Not Provided Sanctions Implementation Reports to the UN

The panel's reports also reveal the essential role played by member states in implementing UN sanctions and that some member states have not been as well informed as others

in working with the panel regarding sanctions implementation. For example, the panel discovered that the Ugandan government had contracted with North Korea to provide police force training. Ugandan government officials purported that they did not realize that UN sanctions prohibited this type of activity, according to a USUN official.

The UN recognized the essential role that member states play when it called upon member states to submit reports on measures or steps taken to implement effectively provisions of specified Security Council resolutions to the committee within 45 or 90 days, or upon request by the committee, of the UN's adoption of North Korea sanctions measures.[47] UNSCRs 1718, 1874, and 2094, adopted in 2006, 2009, and 2013 respectively, call upon member states to report on the concrete measures they have taken in order to effectively implement the specified provisions of the resolutions.[48] For instance, a member state might report on how its national export control regulations address newly adopted UN sanctions on North Korea.

However, more than 80 percent (158) of the UN's 193 member states have not submitted implementation reports in response to these three UNSCRs.[49] Of those 158, 94 have not submitted any implementation reports in response to any of the three UNCRS. Members that have not submitted one or more reports include member states with major international transit points (such as the United Arab Emirates) or that have reportedly been used by North Korea as a foreign intermediary (such as Thailand). The panel has expressed concern in its 2015 final report that 8 years after the adoption of UNSCR 1718, in 2006, a consistently high proportion of member states in some regions have not reported at all on the status of their implementation. It has also reported that some member states have submitted reports that lack detailed information, or were late, impeding the panel's ability to examine and analyze information about national implementation. The panel has also reported that member states should improve their reporting of incidents of noncompliance with sanctions resolutions and inspections of North Korean cargo. Appendix III provides information on the status of member state implementation report submissions.

U.S. officials and representatives of the committee agree that the lack of detailed reports from all member states is an impediment to the UN's effective implementation of its sanctions. Through reviewing these reports, the committee uncovers gaps in member state sanctions implementation which helps the committee identify targets for outreach. The panel notes that the lack of detailed information in implementation reports impedes its ability to examine and analyze information regarding member state implementation

[47] The reporting provisions in USNCR 1718, UNSCR 1874, and UNSCR 2094 differ in the amount of time in which member states are to submit reports on the status of their implementation of the various provisions within their respective UNSCRs. UNSCR 1718 called upon member states to report within 30 days of the resolution's adoption. S.C. Res. 1718, para. 11, U.N. Doc. S/RES/1718 (Oct. 14, 2006). UNSCR 1874 called upon members to report on concrete measures taken to implement paragraph 8 of UNSCR 1718 as well as various provisions within UNSCR 1874 within 45 days of the adoption of the resolution. S.C. Res. 1874, para. 22, U.N. Doc. S/RES/1874 (June 12, 2009). UNSCR 2094 called upon member states to report on concrete measures taken in order to implement effectively the resolution's various provisions within 90 days of the resolution's adoption. S.C. Res. 2094, para. 25, U.N. Doc. S/RES/2094 (Mar. 7, 2013).

[48] S.C. Res. 1718, para. 11, U.N. Doc. S/RES/1718 (Oct. 14, 2006); S.C. Res. 1874, para. 22, U.N. Doc. S/RES/1874 (June 12, 2009); and S.C. Res. 2094, para. 25, U.N. Doc. S/RES/2094 (Mar. 7, 2013).

[49] The United States has complied with UN reporting provisions calling on member states to submit implementation reports. U.S. implementation reports can be viewed on the committee's website, at http://www.un.org/sc/committees/1718/mstatesreports.shtml.

and its challenges. It also states that member state underreporting increases North Korea's opportunities to continue its prohibited activities. The panel will not have the information it needs to completely understand North Korea's evasive techniques if it does not have the full cooperation of member states.

U.S. officials and representatives of the committee told us that many member states lack the technical capacity to enforce sanctions and prepare reports. For instance, representatives of the committee told us that some member states may have weak customs and border patrol systems or export control regulatory structures because of the high resource requirements of these programs. In addition, representatives of the committee stated that some member states may lack awareness of the full scope of North Korea sanctions or may not understand how to implement the sanctions. Moreover, some countries may not make the sanctions a high priority because they believe they are not directly affected by North Korea. In addition, member states that are geographically distant from North Korea or lack a diplomatic or trade relationship with it may not see the need to implement the sanctions, according to representatives of the committee.

The UN has taken some steps to address this impediment. The committee and the panel provide limited assistance to member states upon request in preparing and submitting reports. For example, the committee has developed and issued a checklist template that helps member states indicate the measures, procedures, legislation, and regulations or policies that have been adopted to address various UNSCR measures relevant to member states' national implementation reports. A committee member indicated that the committee developed a list of 25 to 30 member states where outreach would most likely have an impact on reporting outcomes. The panel reported in its 2015 final report that it sent 95 reminder letters to the member states that have not submitted implementation reports, emphasizing the importance of submitting reports and that the panel is available to provide assistance.

Despite the steps the UN has taken to help member states adhere to reporting provisions, the panel's 2015 report continues to identify the lack of member states' reports as an impediment. The panel stated that it is incumbent on member states to implement the measures in the UN Security Council resolutions more robustly in order to counter North Korea's continued violations, and that while the resolutions provide member states with tools to curb the prohibited activities of North Korea, they are effective only when implemented.

State Department officials informed us that the United States has offered technical assistance to some member states for preventing proliferation and implementing sanctions. However, they were unable to determine the extent to which the United States has provided specific assistance aimed at ensuring that member states provide the UN with the implementation reports it needs to assess member state implementation of UN sanctions on North Korea.

Conclusions

North Korea's actions pose threats to the security of the United States and other UN members. Both the United States and the UN face impediments to implementing the sanctions they have imposed in response to these actions. While the United States has recently taken steps to provide more flexibility to impose sanctions, and thereby

possibly impose more sanctions on North Korean persons, the United Nations is seeking to address the challenge posed by many UN member states not providing the UN with implementation information. According to U.S. officials, many member states require additional technical assistance to develop the implementation reports needed by the panel. The lack of implementation reports from member states impedes the panel's ability to examine and analyze information about member state implementation of North Korea sanctions.

Recommendation for Executive Action

GAO recommends the Secretary of State work with the UN Security Council to ensure that member states receive technical assistance to help prepare and submit reports on their implementation of UN sanctions on North Korea.

Agency Comments

We provided a draft of this report to the Departments of State, Treasury, and Commerce for comment. In its written comments, reproduced in Appendix IV, State concurred with our recommendation. Treasury and Commerce declined to provide written comments. State, Treasury, and Commerce provided technical comments, which were incorporated into the draft as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretaries of State, Treasury, and Commerce, the U.S. Ambassador to the United Nations, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9601 or melitot@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Sincerely yours,

[Signature]

Thomas Melito
Director, International Affairs and Trade

Appendix I
United States and United Nations Sanctions Related to North Korea and Iran

The United States and the United Nations (UN) Security Council have imposed a wide range of sanctions against North Korea and Iran as part of their broader efforts to prevent the proliferation of weapons of mass destruction. Table 4 compares the major activities targeted by U.S. and UN sanctions on those countries.

Table 4: Activities Targeted by U.S. and United Nations Sanctions Specific to North Korea and Iran

Targeted activities	North Korea	Iran
Financial transactions with targeted persons	X	X
Weapons of mass destruction proliferation and/or arms and missile transfers	X	X
Human rights abuses/violations	X	X
Censorship		X
Engagement with specific industries (i.e. petroleum, telecommunication)		X
Trade with targeted persons	X	X
Transit of persons engaged in targeted activities	X	X
Evasion of sanctions	X	X

Source: GAO analysis based on U.S. executive orders and laws and United Nations Security Council Resolutions related to North Korea and Iran. | GAO-15-485

Officials from the Department of State, the Department of the Treasury, and other sources identified the following factors that may influence the types of sanctions imposed by the United States and the UN on these countries.

- *Different political systems.* North Korea is an isolated society that is under the exclusive rule of a dictator who controls all aspects of the North Korean political system, including the legislative and judicial processes. Though Iran operates under a theocratic political system, with a religious leader serving as its chief of state, Iranian citizens participate in popular elections for president and members of its legislative branch.
- *Different economic systems.* North Korea has a centrally planned economy generally isolated from the rest of the world. It exports most of its basic commodities to China, its closest ally. Iran, as a major exporter of oil and petrochemical products, has several major trade partners, including China, India, Turkey, South Korea, and Japan.
- *Different social environments.* North Korea's dictatorship tightly controls the activities of its citizens by restricting travel; prohibiting access to the Internet; and controlling all forms of media, communication, and political expression. In contrast, Iranian citizens travel abroad relatively freely, communicate with one another and the world through the Internet and social media, and can hold political protests and demonstrations.

Appendix II
Objectives, Scope, and Methodology

This report (1) identifies the activities that are targeted by U.S. and United Nations (UN) sanctions specific to North Korea, (2) describes how the United States implements its sanctions specific to North Korea and examines the challenges it faces in doing so, and (3) describes how the UN implements its sanctions specific to North Korea and examines the challenges it faces in doing so. In appendix I, we compare U.S. and UN North Korea–specific sanctions with those specific to Iran. (See app. I.)

To address our first objective, we reviewed U.S. executive orders and laws and UN Security Council resolutions issued from 2006 to 2015 with sanctions related to North Korea. We also interviewed officials from the Department of State (State), the Department of the Treasury (Treasury), and the UN to confirm the universe of North Korea–specific sanctions. We also interviewed these officials to determine any other executive orders, laws, or resolutions not specific to North Korea that they have used to impose sanctions on North Korea during this time period. We then analyzed the executive orders, laws, and resolutions to identify the activities targeted by the sanctions.

To address our second objective, we interviewed State and Treasury officials to determine the process that each agency follows to impose sanctions on North Korea and related persons. We also spoke with State, Treasury and Commerce officials to identify the challenges that U.S. agencies face in implementing sanctions related to North Korea. We interviewed Department of Commerce (Commerce) officials to learn about how the U.S. government controls exports to North Korea. We analyzed documents and information from State and Treasury to determine the number of North Korean entities that have been sanctioned since 2006.

To address our third objective, we reviewed UN documents and interviewed UN officials to determine the process that the UN uses to impose sanctions on North Korea and related entities. We reviewed United Nations security resolutions relevant to North Korea, 1718 Committee guidelines and reports, and Panel of Expert guidelines and reports. We interviewed relevant officials at the U.S. State Department and traveled to New York to visit UN headquarters and interview officials from the U.S. Mission to the United Nations and members of the UN 1718 Committee. We interviewed two former members of the Panel of Experts to obtain their views on the UN process for making North Korea sanctions determinations. We also reviewed the 1718 Committee's sanctions list to determine the number of designations the UN has made on North Korean or related entities and the reasons for designating. For examples of how the Panel of Experts has investigated cases of sanctions violations and worked with member states through the investigation process, particularly related to the Cong Chon Gang case, we reviewed the panel's final reports summarizing its investigation findings and interviewed members of the 1718 Committee involved in conducting the investigation. To determine the extent to which member states are submitting reports on their implementation of UN sanctions on North Korea, we examined the 1718 Committee's record of member state implementation reports and interviewed 1718 Committee members. To identify the challenges the UN faces related to member state reporting and the efforts the UN has taken to help member states meet reporting provisions of the UN Security Council resolutions (UNSCR), we interviewed U.S. and UN officials, and reviewed 1718 Committee and Panel of Expert reports and documents. To examine the efforts the UN

has taken to address the lack of member state reporting, we interviewed members of the UN 1718 Committee and reviewed documents outlining UN outreach efforts.

To compare U.S. and UN sanctions specific to North Korea and Iran (see app. I), we reviewed U.S. executive orders, laws, and UN Security Council resolutions with sanctions specific to North Korea and Iran. We analyzed these documents to identify the activities targeted by the sanctions. On the basis of a comprehensive literature review, we developed a list of targeted activities frequently identified in relation to North Korea and Iran sanctions and grouped these activities into high-level categories. To ensure data reliability in categorizing the targeted activities into high-level categories, we conducted a double-blind exercise whereby each member of our team reviewed the activities identified within the U.S. executive orders and laws and UN resolutions for each country and assigned each activity to a high-level category, such as financial transactions with targeted persons. We then compared the results, discussed any differences and reconciled our responses to reach consensus, and developed a matrix to compare the targeted activities for North Korea sanctions with those of Iran sanctions. We interviewed State and Treasury officials to discuss the differences in activities targeted by North Korea and Iran sanctions.

To develop appendix III, on United Nations member state implementation report submissions, we examined the UN 1718 Committee's website record of member state implementation reports. The record of member state implementation reports allowed us to determine the number of member states that have either reported or not reported.

Appendix III
United Nations Member States Implementation Report Submissions, as of April 2015

Country		United Nations Security Council Resolution		
		UNSCR 1718	UNSCR 1874	UNSCR 2094
1.	Afghanistan	Not submitted	Not submitted	Not submitted
2.	Albania	Submitted	Not submitted	Not submitted
3.	Algeria	Submitted	Not submitted	Not submitted
4.	Andorra	Submitted*	Submitted*	Not submitted
5.	Angola	Not submitted	Not submitted	Not submitted
6.	Antigua and Barbuda	Not submitted	Not submitted	Not submitted
7.	Argentina	Submitted	Not submitted	Not submitted
8.	Armenia	Submitted*	Submitted*	Not submitted
9.	Australia	Submitted	Submitted	Submitted
10.	Austria	Submitted	Submitted	Submitted
11.	Azerbaijan	Submitted*	Submitted*	Submitted*
12.	Bahamas	Not submitted	Not submitted	Not submitted
13.	Bahrain, Kingdom of	Submitted	Not submitted	Submitted
14.	Bangladesh	Not submitted	Not submitted	Not submitted
15.	Barbados	Not submitted	Not submitted	Not submitted
16.	Belarus	Submitted	Submitted	Submitted
17.	Belgium	Submitted	Submitted	Submitted
18.	Belize	Not submitted	Not submitted	Not submitted
19.	Benin	Not submitted	Not submitted	Not submitted
20.	Bhutan	Not submitted	Not submitted	Not submitted
21.	Bolivia (Plurinational State of)	Not submitted	Not submitted	Not submitted
22.	Bosnia and Herzegovina	Not submitted	Not submitted	Not submitted
23.	Botswana	Not submitted	Not submitted	Not submitted
24.	Brazil	Submitted*	Submitted*	Submitted
25.	Brunei Darussalam	Submitted	Submitted	Not submitted
26.	Bulgaria	Submitted*	Submitted*	Not submitted
27.	Burkina Faso	Submitted*	Submitted*	Not submitted
28.	Burundi	Not submitted	Not submitted	Not submitted
29.	Cabo Verde	Not submitted	Not submitted	Not submitted

Country		United Nations Security Council Resolution		
		UNSCR 1718	UNSCR 1874	UNSCR 2094
30.	Cambodia	Not submitted	Not submitted	Not submitted
31.	Cameroon	Not submitted	Not submitted	Not submitted
32.	Canada	Submitted	Submitted	Not submitted
33.	Central African Republic	Not submitted	Not submitted	Not submitted
34.	Chad	Not submitted	Not submitted	Not submitted
35.	Chile	Submitted	Submitted	Not submitted
36.	China, People's Republic of	Submitted	Submitted	Submitted
37.	Colombia	Submitted*	Submitted*	Submitted
38.	Comoros	Not submitted	Not submitted	Not submitted
39.	Congo	Not submitted	Not submitted	Not submitted
40.	Costa Rica	Not submitted	Not submitted	Not submitted
41.	Côte d'Ivoire	Not submitted	Not submitted	Not submitted
42.	Croatia	Submitted	Submitted	Not submitted
43.	Cuba	Submitted	Submitted	Not submitted
44.	Cyprus	Submitted*	Submitted*	Submitted*
45.	Czech Republic	Submitted	Not submitted	Not submitted
46.	Democratic People's Republic of Korea	Not submitted	Not submitted	Not submitted
47.	Democratic Republic of the Congo	Not submitted	Not submitted	Not submitted
48.	Denmark	Submitted	Submitted	Submitted
49.	Djibouti	Not submitted	Not submitted	Not submitted
50.	Dominica	Not submitted	Not submitted	Not submitted
51.	Dominican Republic	Not submitted	Submitted	Not submitted
52.	Ecuador	Submitted	Not submitted	Not submitted
53.	Egypt	Submitted*	Submitted*	Not submitted
54.	El Salvador	Not submitted	Not submitted	Not submitted
55.	Equatorial Guinea	Not submitted	Not submitted	Not submitted
56.	Eritrea	Not submitted	Not submitted	Not submitted
57.	Estonia	Submitted*	Submitted*	Not submitted
58.	Ethiopia	Not submitted	Not submitted	Not submitted
59.	Fiji	Not submitted	Not submitted	Not submitted

Country		United Nations Security Council Resolution		
		UNSCR 1718	UNSCR 1874	UNSCR 2094
60.	Finland	Submitted	Submitted	Not submitted
61.	France	Submitted*	Submitted*	Submitted
62.	Gabon	Not submitted	Not submitted	Not submitted
63.	Gambia, The	Not submitted	Not submitted	Not submitted
64.	Georgia	Submitted*	Submitted*	Not submitted
65.	Germany	Submitted	Submitted	Submitted
66.	Ghana	Not submitted	Not submitted	Not submitted
67.	Greece	Submitted	Submitted	Submitted
68.	Grenada	Not submitted	Not submitted	Not submitted
69.	Guatemala	Submitted	Not submitted	Not submitted
70.	Guinea	Not submitted	Not submitted	Not submitted
71.	Guinea Bissau	Not submitted	Not submitted	Not submitted
72.	Guyana	Submitted*	Submitted*	Not submitted
73.	Haiti	Not submitted	Not submitted	Not submitted
74.	Honduras	Not submitted	Not submitted	Not submitted
75.	Hungary	Submitted	Submitted	Not submitted
76.	Iceland	Not submitted	Submitted	Not submitted
77.	India	Submitted	Submitted	Not submitted
78.	Indonesia	Submitted	Not submitted	Not submitted
79.	Iran (Islamic Republic of)	Not submitted	Not submitted	Not submitted
80.	Iraq	Not submitted	Not submitted	Not submitted
81.	Ireland	Not submitted	Submitted	Not submitted
82.	Israel	Submitted	Submitted	Not submitted
83.	Italy	Submitted	Submitted	Not submitted
84.	Jamaica	Not submitted	Not submitted	Not submitted
85.	Japan	Submitted	Submitted	Submitted
86.	Jordan, Hashemite Kingdom of	Submitted*	Submitted*	Submitted*
87.	Kazakhstan	Submitted*	Submitted*	Not submitted
88.	Kenya	Not submitted	Not submitted	Not submitted
89.	Kiribati	Not submitted	Not submitted	Not submitted
90.	Korea, Republic of	Submitted	Submitted	Submitted

Country		United Nations Security Council Resolution		
		UNSCR 1718	UNSCR 1874	UNSCR 2094
91.	Kuwait	Submitted	Not submitted	Not submitted
92.	Kyrgyzstan	Submitted	Not submitted	Not submitted
93.	Lao People's Democratic Republic	Not submitted	Submitted	Not submitted
94.	Latvia	Submitted*	Submitted*	Submitted
95.	Lebanon	Not submitted	Submitted	Not submitted
96.	Lesotho	Not submitted	Not submitted	Not submitted
97.	Liberia	Not submitted	Not submitted	Not submitted
98.	Libya	Not submitted	Not submitted	Not submitted
99.	Liechtenstein	Submitted	Submitted	Not submitted
100.	Lithuania	Submitted*	Submitted*	Submitted
101.	Luxembourg	Submitted*	Submitted*	Submitted
102.	Madagascar	Not submitted	Not submitted	Not submitted
103.	Malawi	Not submitted	Not submitted	Not submitted
104.	Malaysia	Not submitted	Not submitted	Not submitted
105.	Maldives	Submitted	Not submitted	Not submitted
106.	Mali	Not submitted	Not submitted	Not submitted
107.	Malta	Submitted*	Submitted*	Submitted*
108.	Marshall Islands	Submitted	Not submitted	Not submitted
109.	Mauritania	Not submitted	Not submitted	Not submitted
110.	Mauritius	Not submitted	Not submitted	Not submitted
111.	Mexico	Submitted	Submitted	Submitted
112.	Micronesia (Federated States of)	Not submitted	Not submitted	Not submitted
113.	Moldova	Submitted*	Submitted*	Not submitted
114.	Monaco	Not submitted	Submitted	Not submitted
115.	Mongolia	Submitted*	Submitted*	Submitted*
116.	Montenegro	Submitted*	Submitted*	Not submitted
117.	Morocco	Submitted*	Submitted*	Submitted*
118.	Mozambique	Not submitted	Not submitted	Not submitted
119.	Myanmar	Not submitted	Not submitted	Not submitted
120.	Namibia	Not submitted	Not submitted	Not submitted

Country		United Nations Security Council Resolution		
		UNSCR 1718	UNSCR 1874	UNSCR 2094
121.	Nauru	Not submitted	Not submitted	Not submitted
122.	Nepal	Not submitted	Not submitted	Not submitted
123.	Netherlands	Submitted	Submitted	Not submitted
124.	New Zealand	Submitted	Submitted	Submitted
125.	Nicaragua	Not submitted	Not submitted	Not submitted
126.	Niger	Not submitted	Not submitted	Not submitted
127.	Nigeria	Submitted*	Submitted*	Not submitted
128.	Norway	Submitted	Submitted	Not submitted
129.	Oman	Not submitted	Not submitted	Not submitted
130.	Pakistan	Submitted	Submitted	Submitted
131.	Palau	Not submitted	Not submitted	Not submitted
132.	Panama	Submitted*	Submitted*	Not submitted
133.	Papua New Guinea	Not submitted	Not submitted	Not submitted
134.	Paraguay	Not submitted	Not submitted	Not submitted
135.	Peru	Submitted	Submitted	Not submitted
136.	Philippines	Submitted*	Submitted*	Submitted*
137.	Poland	Submitted	Submitted	Not submitted
138.	Portugal	Submitted	Submitted	Not submitted
139.	Qatar	Submitted	Not submitted	Submitted
140.	Romania	Submitted	Submitted	Not submitted
141.	Russian Federation	Submitted	Submitted	Submitted
142.	Rwanda	Not submitted	Not submitted	Not submitted
143.	Saint Kitts and Nevis	Not submitted	Not submitted	Not submitted
144.	Saint Lucia	Not submitted	Not submitted	Not submitted
145.	Saint Vincent and the Grenadines	Not submitted	Not submitted	Not submitted
146.	Samoa	Not submitted	Not submitted	Not submitted
147.	San Marino	Submitted*	Submitted*	Not submitted
148.	Sâo Tome and Principé	Not submitted	Not submitted	Not submitted
149.	Saudi Arabia	Submitted	Submitted*	Submitted*
150.	Senegal	Not submitted	Not submitted	Not submitted
151.	Serbia	Submitted	Submitted	Submitted

Country		United Nations Security Council Resolution		
		UNSCR 1718	UNSCR 1874	UNSCR 2094
152.	Seychelles	Not submitted	Not submitted	Not submitted
153.	Sierra Leone	Not submitted	Not submitted	Not submitted
154.	Singapore	Submitted	Submitted	Submitted
155.	Slovakia	Submitted	Submitted	Not submitted
156.	Slovenia	Submitted	Not submitted	Not submitted
157.	Solomon Islands	Not submitted	Not submitted	Not submitted
158.	Somalia	Not submitted	Not submitted	Not submitted
159.	South Africa	Submitted	Submitted	Not submitted
160.	South Sudan	Not submitted	Not submitted	Not submitted
161.	Spain	Submitted*	Submitted*	Not submitted
162.	Sri Lanka	Submitted	Not submitted	Not submitted
163.	Sudan	Not submitted	Not submitted	Not submitted
164.	Suriname	Not submitted	Not submitted	Not submitted
165.	Swaziland	Not submitted	Not submitted	Not submitted
166.	Sweden	Submitted	Submitted	Submitted
167.	Switzerland	Submitted	Submitted	Submitted
168.	Syrian Arab Republic	Not submitted	Not submitted	Not submitted
169.	Tajikistan	Not submitted	Not submitted	Not submitted
170.	Thailand	Submitted	Submitted	Not submitted
171.	The former Yugoslav Republic of Macedonia	Submitted	Submitted	Not submitted
172.	Timor-Leste	Not submitted	Not submitted	Not submitted
173.	Togo	Not submitted	Not submitted	Not submitted
174.	Tonga	Not submitted	Not submitted	Not submitted
175.	Trinidad and Tobago	Not submitted	Not submitted	Not submitted
176.	Tunisia	Not submitted	Not submitted	Not submitted
177.	Turkey	Submitted	Submitted	Not submitted
178.	Turkmenistan	Submitted	Not submitted	Not submitted
179.	Tuvalu	Not submitted	Not submitted	Not submitted
180.	Uganda	Submitted*	Submitted*	Not submitted
181.	Ukraine	Submitted	Not submitted	Not submitted
182.	United Arab Emirates	Submitted	Not submitted	Not submitted

Country		United Nations Security Council Resolution		
		UNSCR 1718	**UNSCR 1874**	**UNSCR 2094**
183.	United Kingdom	Submitted	Submitted	Submitted
184.	United Republic of Tanzania	Not submitted	Not submitted	Not submitted
185.	United States of America	Submitted	Submitted	Submitted
186.	Uruguay	Not submitted	Not submitted	Not submitted
187.	Uzbekistan	Submitted*	Submitted*	Not submitted
188.	Vanuatu	Not submitted	Not submitted	Not submitted
189.	Venezuela (Bolivarian Republic of)	Not submitted	Not submitted	Not submitted
190.	Viet Nam, Socialist Republic of	Submitted	Submitted	Submitted
191.	Yemen	Not submitted	Not submitted	Not submitted
192.	Zambia	Not submitted	Not submitted	Not submitted
193.	Zimbabwe	Not submitted	Not submitted	Not submitted
United Nations nonmember observers		**UNSCR 1718**	**UNSCR 1874**	**UNSCR 2094**
1	European Union (Finland)	Submitted	Not submitted	Not submitted

Source: GAO analysis of UN information. | GAO-15-485

Note: United Nations member state implementation reports can be viewed on the committee's website, at: http://www.un.org/sc/committees/1718/mstatesreports.shtml. (*) indicates that the submission was part of a combined implementation report.

Appendix IV
Comments from the Department of State

United States Department of State
Comptroller
Washington, DC 20520

MAY 01 2015

Dr. Loren Yager
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "NORTH KOREA SANCTIONS: U.S. Has Increased Flexiblity to Impose Sanctions, but UN is Impeded by a Lack of Member State Reports" GAO Job Code 321035.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Thomas Zarzecki, Foreign Affairs Officer, Office of Counterproliferation Initiatives, Bureau of International Security and Nonproliferation at (202) 647-7594.

Sincerely,

Christopher H. Flaggs

Enclosure:
As stated.

cc: GAO – Thomas Melito
ISN – Vann Van Diepen
State/OIG - Norman Brown

Department of State Comments on GAO Draft

NORTH KOREA SANCTIONS: U.S. Has Increased Flexibility to Impose Sanctions, but UN Is Impeded by a Lack of Member State Reports
(GAO-15-485, GAO Code 321035)

The Department appreciates the opportunity to comment on the GAO draft report entitled *"North Korea Sanctions: U.S. Has Increased Flexibility to Impose Sanctions, but UN Is Impeded by a Lack of Member State Reports."*

The Department of State agrees with the recommendation and already works closely with many other UN Member States on the implementation of the North Korea-related UN Security Council resolutions (UNSCRs), and strongly urges all States to submit their implementation reports called for in the UNSCRs. Submission of a national implementation report is, however, only one action among many that a State can and should take to strengthen is implementation of the UNSCRs.

Appendix V
GAO Contact and Staff Acknowledgments

GAO Contact

Thomas Melito, (202) 512-9601 or melitot@gao.gov

Staff Acknowledgments

In addition to the contact named above, Pierre Toureille (Assistant Director), Leah DeWolf, Christina Bruff, Mason Thorpe Calhoun, Tina Cheng, Karen Deans, Justin Fisher, Toni Gillich, Michael Hoffman, and Grace Lui made key contributions to this report.

E. THE MILITARY AND LAW ENFORCEMENT

COMMENTARY

by
Douglas C. Lovelace, Jr.

Section E concludes this volume with a presentation of three documents that address military and civilian law enforcement interactions necessitated by hybrid warfare. The first document is a June 10, 2015, GAO report on Testimony before the Subcommittee on Emergency Preparedness, Response, and Communications of the Committee on Homeland Security of the House of Representatives, entitled *DOD Is Taking Action to Strengthen Support of Civil Authorities*. As its title suggests, the document reports on DOD's improvements in strategic planning for support to civil authorities, its efforts to enhance interagency coordination, and improvement in its support capabilities and capacity. The report states that DOD has improved its ability to support civil authorities but more improvement is possible and needed.

We include this report in this volume to demonstrate once again that the scope of hybrid warfare encompasses even the use of the U.S. armed forces inside the United States. We are often reminded that the Posse Comitatus Act precludes the use of military forces for domestic law enforcement. While that is generally true, there are important exceptions, such as the provisions of the Insurrection Act. Additionally, as hybrid warfare runs the risk of bringing belligerents to U.S. shores and also involves what are commonly known as "home-grown terrorists," the use of the U.S. armed forces to maintain domestic law and order could well increase.

The next document offered in Section E is an August 28, 2014, Congressional Research Service report on *The "1033 Program," Department of Defense Support to Law Enforcement*. The 1033 Program permits the transfer of military equipment, including arms and other combat weapons systems, to civilian law enforcement agencies. The report correctly notes that the program is widely subscribed with some 11,000 agencies participating across the country. The program has become very controversial. With law enforcement agencies receiving the same equipment military personnel use to attack and defeat enemies in war and the training on how to use it, many have asked openly whether law enforcement agencies are becoming de facto military units. This perception has been reinforced by recent videos of law enforcement officers employing tactics and equipment in ways that are very similar to the ways in which soldiers would in subduing an enemy force. Again, this is further evidence that hybrid warfare transcends U.S. borders and might well include law enforcement personnel as participants. Such is the response to the hybrid and Gray Zone threats that are increasingly defining the international and national security environments.

The final document in Section E is a short December 2, 2014, Congressional Research Service "CRS Insights" report on *The "Militarization" of Law Enforcement and the Department of Defense's "1033 Program*." We conclude Section E with this piece to demonstrate the negative impact and deleterious effect hybrid warfare can have on the fabric of U.S. society when it finds its way into domestic law enforcement. One of the major strengths of U.S. society is its capacity for self-correction. Nonetheless, the hybrid threat has penetrated U.S. borders and must be countered. However, the merging of the military with law enforcement could well be a poison pill.

DOCUMENT NO. 11

CIVIL SUPPORT: DOD IS TAKING ACTION TO STRENGTHEN SUPPORT OF CIVIL AUTHORITIES

Statement of Joseph W. Kirschbaum, PhD
Director, Defense Capabilities and Management

United States Government Accountability Office

Testimony Before the Subcommittee on Emergency Preparedness, Response, and Communications, Committee on Homeland Security, House of Representatives

June 10, 2015

GAO-15-686T

GAO
Highlights

Highlights of GAO-15-686T, a testimony before the Subcommittee on Emergency Preparedness, Response, and Communications, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Threats to the homeland and major disasters and emergencies, such as hurricanes and wildfires, are frequently unpredictable or occur with little or no notice. DOD is often expected to play a prominent role supporting civil authorities and must be prepared to provide rapid response when called upon during disasters and declared emergencies (both natural and man-made). DOD also must provide support for restoring public health and services and civil order; support for national special security events; and periodic planned support. DOD provides this support to the American people through its defense support of civil authorities mission.

In this statement, GAO describes progress DOD has made in implementing recommendations to strengthen (1) DOD's strategy, plans, and guidance; (2) interagency

coordination; and, (3) capabilities to support civil authorities. This testimony is primarily based on GAO products issued from March 2010 through December 2014 that examined DOD's support of civil authorities mission. In June 2015 GAO obtained selected updates about DOD's support of civil authorities mission.

What GAO Recommends

GAO previously made recommendations to help DOD address management challenges or gaps in guidance regarding support of civil authorities. In response, the agency has taken some steps and plans to do more.

For more information, contact Joseph Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

What GAO Found

The Department of Defense (DOD) has taken action to address GAO's prior recommendations to strengthen its strategy, plans and guidance for support of civil authorities. As GAO has reported, clear, current, and complete strategies, plans, and guidance are important for reflecting the direction of the department's leadership, defining DOD policies and responsibilities, and sharing practices that could facilitate effective support of civil authorities. In October 2012, GAO found DOD had not developed guidance for the use of dual-status commanders (active-duty military or National Guard officers who were authorized to command both state and federal personnel) for incidents affecting multiple states and territories. For example, DOD had no specific criteria and conditions for when and how state governors and the Secretary of Defense would mutually appoint a commander. In September 2013, GAO found that DOD did not have a clear command-and-control structure for managing complex catastrophes across multiple states because DOD had not identified roles, responsibilities, and relationships among command elements. GAO recommended in both reports that DOD update and implement better guidance. DOD has partially addressed GAO's recommendations by updating its strategy and guidance, and the department is drafting an instruction on dual-status commanders.

DOD also has taken action to address GAO's prior recommendations to strengthen the department's interagency coordination. It is critical that DOD coordinate and synchronize its civil support mission to engage with a broad range of interagency partners it may need to support, such as the Federal Emergency Management Agency (FEMA) and Customs and Border Protection. Previously, GAO reported on three areas DOD can focus on to enhance interagency coordination: clearly define roles and responsibilities, communicate DOD's approach toward interagency partners, and implement key practices for managing liaisons with partners. GAO found that roles and responsibilities for support to law enforcement—including Joint Task Force-North, which provides civil support along U.S. borders—were unclear. GAO also found that DOD did not have complete situational awareness of 110 liaisons detailed to the Department of Homeland Security headquarters. To improve interagency coordination, GAO recommended

that DOD issue and update civil-support guidance. Subsequently, DOD addressed GAO's recommendations by issuing guidance and other documents, such as the 2011 Interagency Partner Guide.

Additionally, DOD has taken action to address GAO's prior recommendations to improve its identification of capabilities for support of civil authorities. In the 2014 *Quadrennial Defense Review,* DOD notes that the key pillar of protecting the homeland includes sustaining capabilities to assist U.S. civil authorities. In 2013, GAO found two combatant commands had not identified civil-support capabilities because they were waiting until FEMA completed planning efforts in 2018. GAO recommended that DOD develop an interim set of specific capabilities that could be provided to prepare for and respond to complex catastrophes. DOD concurred with GAO's recommendation and DOD officials reported as of June 2015 that Northern Command and Pacific Command had updated their plans to incorporate complex catastrophes, including identifying capabilities that would be available to the lead federal agency during such an event.

Chairman McSally, Ranking Member Payne, and Members of the Subcommittee:

I am pleased to be here today to discuss progress and challenges in the Department of Defense's (DOD) efforts to serve the American people through its defense support of civil authorities (DSCA) mission.[1] The United States continues to face an uncertain, complex security environment with the potential for major disasters and emergencies, such as Hurricane Sandy in 2012. The 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities* recognizes DOD is often expected to play a prominent role supporting civil authorities and must be prepared to provide rapid response when called upon.[2] DOD must coordinate with a number of other agencies on its civil support mission, which include providing support during disasters and declared emergencies (both natural and man-made); providing support for restoring public health and services and civil order; providing support for national special security events; and periodic planned support. Examples of such DOD coordination with civil authorities include aiding the identification and interdiction of suspected transnational criminal organizations' activities conducted within and along the approaches to the continental United States; assisting the Federal Emergency Management Agency (FEMA) during the annual hurricane season; assisting the Department of Transportation after the I-35 bridge collapse in Minnesota in 2007; and supporting the U.S. Secret Service regarding Presidential inaugurations. In these and other events, DOD offered a broad array of resources that were developed for its warfighting mission but were brought to bear when civilian-response capabilities were overwhelmed or exhausted—or in instances where DOD offered unique capabilities.

In an effort to facilitate defense support of civil authorities across the nation and at all organizational levels, DOD has assigned responsibilities within the Office of the Secretary of Defense (such as the Office of the Assistant Secretary of Defense for

[1] Defense support of civil authorities is support provided by federal military forces, DOD civilians, DOD contract personnel, DOD component assets, and, in certain circumstances, National Guard forces in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.

[2] DOD, *Strategy for Homeland Defense and Defense Support of Civil Authorities* (February 2013).

Homeland Defense and Global Security),[3] the Joint Chiefs of Staff, various combatant commands (such as Northern Command and Pacific Command), the National Guard Bureau, the U.S. Army Corps of Engineers, the Defense Logistics Agency, joint task forces (such as Joint Task Force-North),[4] the intelligence agencies (such as the National Geospatial-Intelligence Agency and the Defense Intelligence Agency), and regional interagency liaisons (such as the Defense Coordinating Officers and Emergency Preparedness Liaison Officers).[5]

My testimony is based on reports we issued from March 2010 through December 2014 that examined DOD's DSCA mission, and discusses DOD's progress in implementing recommendations that we made to strengthen (1) DOD's strategy, plans, and guidance documents; (2) interagency coordination; and, (3) capabilities to support civil authorities.[6]

This statement includes selected updates that we conducted in June 2015 on DOD's DSCA mission. Our reports contained information that we obtained from reviewing and analyzing relevant DOD documents, including the 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities*; *The DOD Cyber Strategy* from 2015; Northern Command and Pacific Command planning documents; DOD directives, instructions, and doctrine; and Northern Command capability assessments. We also conducted interviews with DOD officials within the Office of the Secretary of Defense, Joint Staff, combatant commands, military services, defense agencies, and Reserve officials. We also conducted interviews with other federal officials from organizations such as the Department of Homeland Security (DHS), FEMA, Customs and Border Protection, Immigration and Customs Enforcement, Federal Bureau of Investigation, Drug Enforcement Agency, Centers for Disease Control and Prevention, Animal and Plant Health Inspection Service, and officials located in the El Paso Intelligence Center. More detailed information about our scope and methodology can be found in our reports.

---

[3] In January 2015, the Office of the Under Secretary of Defense for Policy reorganized its missions and renamed the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs as the Assistant Secretary of Defense for Homeland Defense and Global Security. For the purpose of consistency, we will refer to the position in this report as the Assistant Secretary of Defense for Homeland Defense.

[4] Joint Task Force-North, formerly referred to as Joint Task Force-6, was created in 1989 to serve as the planning and coordinating operational headquarters to support local, state, and federal law enforcement agencies within the southwest border region to counter the flow of illegal drugs into the United States. In the aftermath of the September 11, 2001, terrorist attacks on the United States, the command was officially renamed Joint Task Force-North and its mission was expanded to include providing homeland security support to the nation's federal law enforcement agencies.

[5] A Defense Coordinating Officer is a DOD single point of contact for domestic emergencies who is assigned to a joint field office to validate requests for assistance, forward mission assignments through proper channels to the appropriate military organizations, and assign military liaisons, as appropriate, to activated emergency support functions. An Emergency Preparedness Liaison Officer is a senior reserve officer who represents their service at the appropriate joint field office conducting planning and coordination responsibilities in support of civil authorities. See Joint Publication 3-28, *Defense Support to Civil Authorities* (Jul. 31, 2013).

[6] This statement is based on the following reports that are cited throughout and include GAO, *Emergency Preparedness: Opportunities Exist to Strengthen Interagency Assessments and Accountability for Closing Capability Gaps*, GAO-15-20 (Washington, D.C.: Dec. 4, 2014); *Civil Support: Actions Are Needed to Improve DOD's Planning for a Complex Catastrophe*, GAO-13-763 (Washington, D.C.: Sep. 30, 2013); *Homeland Defense: DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance*, GAO-13-128 (Washington, D.C.: Oct. 24, 2012); *Homeland Defense: DOD Can Enhance Efforts to Identify Capabilities to Support Civil Authorities during Disasters*, GAO-10-386 (Washington, D.C.: Mar. 30, 2010); and, *Homeland Defense: DOD Needs to Take Actions to Enhance Interagency Coordination for Its Homeland Defense and Civil Support Missions*, GAO-10-364 (Washington, D.C.: Mar. 30, 2010).

For the updates, we collected information from DOD officials on actions the department has taken to address findings and recommendations made in our prior reports. The work upon which this testimony is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DOD Continues to Take Action to Strengthen Its DSCA Strategy, Plans, and Guidance

DOD has and continues to take action to address our prior recommendations to strengthen its DSCA strategy, plans, and guidance. As we have previously reported, clear, current, and complete strategies, plans, and guidance documents are important for reflecting the direction of the departments' civilian and military leadership, defining DOD and its components' policies and responsibilities, and sharing practices that could facilitate effective support of civil authorities. In 2005, DOD issued its first *Strategy for Homeland Defense and Civil Support*.[7] In four reports we issued in 2010 through 2013, we found that DOD's DSCA strategies and guidance were outdated, not fully integrated, or were not comprehensive.[8] Since 2010, DOD has taken action to address many of our findings and recommendations. For example:

- **DOD updated its strategy and doctrine for civil support.** In 2010, and then again in 2012, we found that DOD's 2005 *Strategy for Homeland Defense and Civil Support* had not been updated to reflect the current environment in which DOD supports civil authorities. For example, while the strategy primarily discusses DOD's DSCA mission in the context of the department's response to a weapon of mass destruction—DOD's primary focus after the 2001 terrorist attacks—it did not address the breadth of DSCA missions that DOD must be prepared to support subsequent to Hurricane Katrina in 2005. Based on our recommendation that DOD should update its strategy, in February 2013 DOD issued an updated *Strategy for Homeland Defense and Defense Support of Civil Authorities*. In this update, DOD acknowledged that national security threats, hazards, vulnerabilities, strategic guidance, and political and economic factors had evolved since the 2005 strategy, and recognized that its support to civil authorities included a broader set of missions—to include catastrophic natural or man-made disasters, pre-planned National Special Security Events (like summits and high-profile sports events), cyberattacks, and the southwest border counterdrug efforts. We also reported in 2012 that DOD had not updated its joint publication for DSCA and recommended that the department needed to do so. DOD agreed with our recommendation and in July 2013, DOD updated its joint publication for Defense Support for Civil Authorities.[9] In this update, among other things, DOD described more fully the *National Response Framework*, which is a framework based on a tiered, graduated response to major

[7] DOD, *Strategy for Homeland Defense and Civil Support* (June 2005).

[8] GAO-13-763, GAO-13-128, GAO-10-364, and GAO-10-386.

[9] Joint Publication 3-28, *Defense Support of Civil Authorities*, (July 31, 2013).

disasters and emergencies where incidents are managed at the lowest jurisdictional level and are supported by additional response capabilities, as needed.[10]

- **DOD has reported that it has updated its DSCA plans.** In September 2013,[11] we found that DOD did not have a clear command-and-control structure for federal military services during complex catastrophes.[12] We found that DOD had not identified the roles, responsibilities, and relationships among command elements that may be involved in responding to such incidents across multiple states. This issue was illustrated by events such as National Level Exercise 2011 that examined DOD's response to a complex catastrophe. Similarly, DOD's after-action reports on Hurricane Sandy in 2012 found that the command-and-control structure for federal military forces was not clearly defined, resulting in the degradation of situational awareness and unity of effort, and the execution of missions without proper approval. Northern Command officials agreed with our findings and stated that they would address this issue and the associated recommendation we made in our report by updating their DSCA plans. As of June 2015, DOD reported that Northern Command and Pacific Command had updated their DSCA plans to address our recommendation.
- **DOD implementation guidance on the use of dual-status commanders is in development.** DOD established the dual-status commander structure—active-duty military or National Guard officers who command state and federal responses to civil-support incidents and events—and has used this structure for certain events.[13] For example, DOD used the dual-status commander structure for the 2012 Colorado wildfire response and the Hurricane Sandy response. In October 2012, we reported that DOD had not developed guidance for the use of dual-status commanders for incidents affecting multiple states and territories.[14] For example, DOD had not developed specific criteria and conditions for when and how state governors and the Secretary of Defense would mutually appoint a commander. Consequently, we recommended and DOD concurred that the department develop implementation guidance on the use of dual-status commanders. In June 2015, Northern Command officials reported that an instruction about dual-status commanders was being drafted in coordination with DOD, Northern Command, and the National Guard Bureau.

[10] The *National Response Framework* is a guide to how the nation responds to all types of disasters and emergencies. It is built on scalable, flexible, and adaptable concepts identified in the National Incident Management System to align key roles and responsibilities across the nation. This framework describes specific authorities and best practices for managing incidents that range from the serious but purely local to large-scale terrorist attacks or catastrophic natural disasters. The *National Response Framework* describes the principles, roles and responsibilities, and coordinating structures for delivering the core capabilities required to respond to an incident and further describes how response efforts integrate with those of the other mission areas.

[11] GAO-13-763.

[12] DOD has defined a complex catastrophe as a natural or man-made incident, including cyberspace attack, power grid failure, and terrorism, which results in cascading failures of multiple interdependent, critical, life-sustaining infrastructure sectors and causes extraordinary levels of mass casualties, damage, or disruption severely affecting the population, environment, economy, public health, national morale, response efforts, and/or government functions.

[13] Dual-status commanders are military commanders who serve as an intermediate link between the separate chains of command for state and federal forces.

[14] GAO-13-28.

- **DOD has agreed to take steps to align cyber-support roles and responsibilities.** In October 2012, we found that DOD had not updated its DSCA guidance, such as joint doctrine, to ensure that it was consistent with national plans and preparations for domestic cyber incidents.[15] We recommended that DOD align guidance on preparing for and responding to domestic cyber incidents with national-level guidance to include roles and responsibilities. DOD partially concurred with this recommendation. However, the department has not yet taken action that meets the intent of the recommendation.

DOD Has Taken Action to Strengthen Interagency Coordination for Support of Civil Authorities

DOD has and continues to take action to address our prior recommendations to strengthen the department's interagency coordination for support of civil authorities. As numerous events within the homeland in the last decade have pointed out, it is critical that DOD coordinate, integrate, and synchronize its DSCA mission with a broad range of interagency partners that the department may need to support. Such partners can include FEMA, Federal Bureau of Investigation, Customs and Border Protection, Animal and Plant Health Inspection Service, and the Centers for Disease Control and Prevention. As we have previously reported, there are three key areas that DOD needs to focus on to enhance and institutionalize its interagency coordination efforts. DOD has since taken action to address these areas:

- **DOD has better defined interagency roles and responsibilities.** Previous GAO work, the *National Response Framework*, and DOD strategic guidance identify the need for clearly defined roles and responsibilities to enhance interagency coordination.[16] In our 2010 review of DOD's interagency coordination efforts, we found that the key documents used to define roles and responsibilities were outdated, not fully integrated, or were not comprehensive.[17] We found that DOD's series of civil-support policies and guidance, such as a 1997 DOD directive on military assistance to civil authorities,[18] were outdated and did not reflect changes that occurred subsequent to their issuance. For example, the guidance documents did not refer to DHS, the Office of the Assistant Secretary of Defense for Homeland Defense, Northern Command, or roles and responsibilities under the *National Response Framework*. Similarly, we found that roles and responsibilities for support to law enforcement—including Joint Task Force-North, which provides defense support of civilian law enforcement agencies along U.S. borders—were unclear as were the roles and responsibilities between the Assistant Secretary of Defense for Health Affairs and the Assistant Secretary of Defense for Homeland Defense. Consequently, we recommended and DOD concurred that the department should update key documents that outline roles and responsibilities. Subsequently, DOD

[15] GAO-13-28.

[16] DHS, *National Response Framework, Second Edition (May 2013)*; DOD, Joint Publication 3-08, *Interorganizational Coordination During Joint Operations* (June 24, 2011); GAO-10-364; DOD, *National Defense Strategy* (June 2008);and GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

[17] GAO-10-364.

[18] DOD Directive 3025.15, *Military Assistance to Civil Authorities* (Feb. 18, 1997).

has, for the most part, issued new guidance documents or updated older guidance to better define roles and responsibilities within the department for interagency coordination.

- **DOD has issued an interagency partner guide.** DOD's joint doctrine on interagency coordination and support of civil authorities notes that a unified "whole-of-government" approach to national security issues requires federal partner agencies to understand core competencies, roles, and missions and that sharing information is critical for the success of interagency coordination between federal agencies.[19] To support interagency coordination on DSCA, DOD has taken action to communicate with its federal partners through conferences and other forums and multiple documents. In our 2010 review of DOD's interagency coordination efforts, we found that DOD's approach to communicating with federal partners could be improved, and the department had not clearly identified the roles and responsibilities and day-to-day coordination processes with its federal partners through a single, readily accessible source.[20] Specifically, DOD, DHS, and the Department of Justice officials told us that the benefits gained through interagency forums, such as Homeland Security Council meetings and annual National Interagency Fire Center conferences, are transient because they depend on personnel who rotate out of their positions frequently. The National Interagency Fire Center had addressed this challenge by creating a partner handbook that identified key information. DOD had not developed a similar vehicle for institutionalizing its information sharing efforts so that federal partners could maintain knowledge and have readily accessible information about key issues, such as the different DOD entities that have DSCA missions. For those cases where DOD internally documented its missions, roles, and responsibilities, we found the information was dispersed among multiple sources; also, the documents may not have always been readily accessible to federal partners, and they may have been written in a manner that led to unclear expectations. Therefore, we recommended that DOD develop and issue a partner guide that identifies the roles and responsibilities of DOD entities, processes, and agreed-upon approaches for interagency coordination for homeland defense and civil-support efforts. DOD concurred with our recommendation and, in November 2011, issued its *Defense Support of Civil Authorities Interagency Partner Guide*.
- **DOD has taken action to implement key practices for managing some liaisons the department exchanges with its federal partners.** Prior GAO reports and DOD guidance recognize that leading organizations employ key practices for effective and efficient workforce planning, such as situational awareness, staffing-needs assessments, position descriptions, training, and performance assessments.[21] However, in our 2010 report, we found that DOD had not implemented

[19] Joint Publication 3-28, *Defense Support of Civil Authorities* (July 31, 2013); and Joint Publication 3-08, *Interorganizational Coordination During Joint Operations* (June 24, 2011).

[20] GAO-10-364.

[21] DOD Instruction 1315.18, *Procedures for Military Personnel Assignments* (Jan. 12, 2005); DOD Instruction 1400.25, *DOD Civilian Personnel Management System* (Nov. 18, 2008); DOD Instruction 1000.17, *Detail of DOD Personnel to Duty Outside the Department of Defense* (Apr. 16, 2008); GAO, *Human Capital: Key Principles for Effective Strategic Workforce Planning*, GAO-04-39 (Washington, D.C.: Dec. 11, 2003; and GAO, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002).

such key practices.[22] For example, DOD did not have complete situational awareness of all the liaisons detailed to its interagency partners. According to DOD records, in 2009, there were only 2 DOD personnel at DHS headquarters—yet an informal survey by the representative for the Office of the Assistant Secretary of Defense for Homeland Defense to DHS found that more than 110 DOD personnel, from a variety of DOD entities, were working at DHS as liaisons, subject-matter experts, or in other capacities.[23] Therefore, we recommended and DOD agreed that DOD develop and issue additional workforce management policy and guidance regarding DOD liaisons to other federal agencies, as well as other federal agencies' liaisons to DOD. In October 2013, the Deputy Secretary of Defense and the Acting Deputy Secretary of Homeland Security signed an updated memorandum of agreement that outlines ways in which DOD and DHS will incorporate key practices for managing liaisons in the national capital region.

DOD Has Taken Action to Identify Needs and Address Capability Gaps Regarding Its Support of Civil Authorities

In response to our prior recommendations, DOD has taken action to identify needs and address capability gaps for its DSCA mission. In the 2014 *Quadrennial Defense Review*, DOD notes that the key pillar of protecting the homeland includes sustaining capabilities to assist U.S. civil authorities in protecting U.S. airspace, shores, and borders, and in responding effectively to domestic man-made and natural disasters.[24] In 2008, DOD conducted a capabilities-based assessment of its homeland defense and civil support missions to enable improvements for DOD homeland defense and civil-support policy, evaluate existing DOD capabilities and identify capability gaps, improve DOD's integration with interagency mission partners, and recommend further action to promote future capability development. In 2010, we found that DOD and DHS had undertaken initiatives to address gaps in strategic planning that should assist DOD in identifying its capability requirements for the DSCA mission.[25] For example, DOD and DHS issued catastrophic plans for responding to and recovering from a category 4 hurricane in Hawaii. In addition, DHS had established a pilot initiative entitled Task Force for Emergency Readiness pilot initiative that sought to integrate federal and state planning efforts for catastrophic events, which in turn would assist DOD in determining the capabilities it may be asked to provide. However, we found that DOD's DSCA policy and guidance was outdated, which limited DOD's ability to address capability gaps. We therefore made a recommendation and DOD concurred that the department should update its DSCA guidance. Since then, DOD has updated or replaced several DSCA

[22] GAO-10-364.

[23] In responding to a draft of this statement, DOD stated that, according to a 2004 DOD-DHS memorandum of agreement on personnel exchange, there were at least 38 DOD personnel detailed to (or assigned as liaisons at) DHS headquarters and 86 DoD personnel to DHS, in general. However, during the audit, DOD documents and officials reflect that DOD's numbers were inaccurate and that the officials did not have an exact count on the number of DOD personnel located at DHS headquarters or throughout the DHS organization.

[24] DOD, *Quadrennial Defense Review 2014* (Mar. 4, 2014).

[25] GAO-10-386.

guidance documents, such as DOD Directive 3025.18.[26] By updating this guidance, DOD addressed our recommendation and DOD is in a better position to address remaining capability gaps.

Additionally, we found in 2013 that DOD had not taken all of the necessary steps to identify capabilities for DSCA.[27] Specifically, we found that Northern Command and Pacific Command were updating their DSCA plans to include a scenario for a complex catastrophe; however, the commands delayed identification of capabilities that could be provided to execute the plans in light of FEMA's plan to complete its regional planning efforts in 2018. We recommended that the commanders work through the defense coordinating officers to develop an interim set of specific capabilities that could be provided to prepare for and respond to complex catastrophes while FEMA completes its plans. DOD concurred with our recommendation and, in May 2014, according to DOD officials, Northern Command and Pacific Command had updated their plans to incorporate complex catastrophes, including identifying capabilities that would be available to the lead federal agency during such an event. Specifically, DOD officials told us, in June 2015, that planning had been completed, covering issues such as complex catastrophes; wildland firefighting; and chemical, biological, radiological, and nuclear response. Additionally, DOD officials told us that future planning efforts will include additional branch plans addressing issues such as pandemic influenza and infectious diseases and civil disturbance operations.

Under the *National Response Framework*, the U.S. Army Corps of Engineers serves as the coordinator for the 'Public Works and Engineering' emergency support function—1 of 14 emergency support functions that serve as the federal government's primary coordinating structure for building, sustaining, and delivering response capabilities.[28] The U.S. Army Corps of Engineers, in its emergency support function coordinator role, is responsible for engaging in appropriate planning and preparedness activities, which could include establishing capability requirements, cataloguing current capabilities, and conducting capability gap analyses that might be needed if the federal government is asked to support local, state, tribal, territorial, and insular area government response operations during a disaster. In a recent assessment of the federal preparedness to respond to no-notice catastrophic disasters, such as improvised nuclear device attacks and major earthquakes, we found that the U.S. Army Corps of Engineers had taken an insular approach to identifying, cataloguing, and analyzing gaps for public works and engineering capabilities.[29] Since we concluded that the U.S. Army Corps of Engineers' actions—as well as actions by other non-DOD agencies that serve as coordinators for different emergency support functions—were attributable to unclear guidance, and

[26] DOD Directive 3025.18, *Defense Support of Civil Authorities* (DSCA) (Dec. 29, 2010, incorporating change 1, Sep. 21, 2012).

[27] GAO-13-763.

[28] The *National Response Framework* states that the Secretary of Homeland Security is to ensure that overall federal preparedness actions are unified, complete, and synchronized to prevent unfilled gaps or seams in the federal government's efforts to respond to all hazards. The emergency support functions are organized by specific functional areas for the most frequently needed capabilities during an emergency—including communications, medical services, and search and rescue—and are designed to coordinate the provision of related assets and services by federal departments and agencies. See DHS, *National Response Framework, Second Edition (May 2013).*

[29] GAO-15-20.

recommended that FEMA issue supplemental guidance to the agencies that serve as coordinators for the different emergency support functions.[30] FEMA concurred with this recommendation and estimated that it would complete this supplemental guidance by June 30, 2015.

In conclusion, threats to the homeland and major disasters and emergencies, such as cyber attacks and earthquakes, frequently are unpredictable or occur with little or no notice. DOD's 2014 *Quadrennial Defense Review* emphasizes protecting the homeland, including deterring and defeating attacks on the United States and supporting civil authorities in mitigating the effects of potential attacks and natural disasters, as the first of the defense strategy's three pillars. DOD has made significant progress in improving strategy, plans, and guidance; interagency coordination; and capabilities needed for DSCA. Our work also shows that there remains room for improvement and that DOD recognizes this and intends to fully address the remaining recommendations from our prior reports. We continue to believe that their implementation will buttress the advanced planning and interagency coordination effort DOD requires to support civil authorities in responding to the myriad threats and challenges we face. On that note, looking ahead, we will continue to monitor and evaluate (1) DOD's cyber civil support, (2) the status of the homeland response forces, (3) DOD's preparedness for civil support in the event of a pandemic, and (4) coordination with federal agencies to counter improvised explosive devices in the United States.

Chairman McSally, Ranking Member Payne, and members of the subcommittee, this concludes my prepared statement. I am happy to answer any questions you may have.

GAO Contacts and Staff Acknowledgments

If you or your staff have any questions about this statement, please contact me at (202) 512-9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this statement include Tommy Baril (Assistant Director), Jennifer Andreone, Gina Flacco, Brent Helt, Amber Lopez Roberts, Randy Neice, Richard Powelson, and Bethann Ritter Snyder. Elizabeth Morris, Terry Richardson, Jennifer Spence, Michael Willems, and John Van Schaik provided additional support.

[30] FEMA serves as the chair of the Emergency Support Function Leadership Group.

DOCUMENT NO. 12

THE "1033 PROGRAM," DEPARTMENT OF DEFENSE SUPPORT TO LAW ENFORCEMENT

CRS Report R43701

Daniel H. Else
Specialist in National Defense

August 28, 2014

Summary

The United States has traditionally kept military action and civil law enforcement apart, codifying that separation in the Posse Comitatus Act of 1878. On the other hand, Congress has occasionally authorized the Department of Defense (DOD) to undertake actions specifically intended to enhance the effectiveness of domestic law enforcement through direct or material support.

One such effort is the so-called "1033 Program," named for the section of the National Defense Authorization Act (NDAA) of 1997 that granted permanent authority to the Secretary of Defense to transfer defense material to federal and state agencies for use in law enforcement, particularly those associated with counter-drug and counter-terrorism activities.

The 1997 act was preceded by 1988 legislation that expanded DOD's role in the interdiction of illicit drug trafficking. That was soon followed by temporary authority to transfer excess defense material, including small arms and ammunition, from excess DOD stocks to law enforcement agencies for use in counter-drug activities. This could be done at no cost to the receiving agency. The 1997 NDAA expanded that authority to include counter-terrorism activities and made it permanent. It is codified as 10 U.S.C. §2576a.

The 1033 Program is administered by the Law Enforcement Support Office (LESO) of the Defense Logistics Agency (DLA). Under it, local and state law enforcement agencies may apply to DLA to participate. DLA requires the governor of the state to execute a Memorandum of Agreement (MOA) and appoint a state 1033 Program coordinator, who is responsible for ensuring that the program is properly administered within the state and that appropriate property records are maintained. Approved agencies may request material from DLA through their state coordinators. The LESO retains final approval

authority over the types and quantities of material transferred from DOD excess stocks to the agencies. Any material requiring demilitarization before being released to the public must be returned to DLA when no longer needed by the receiving law enforcement agency.

LESO states that 11,000 agencies nationwide are currently registered and that 8,000 of them use material provided through the 1033 Program.

Department of Defense Support to Law Enforcement

American tradition has long maintained a distinct separation between military force and civil law enforcement. Nevertheless, federal troops were commonly used to enforce civil law during the years immediately after the Civil War, particularly in the states of the former Confederacy. The Posse Comitatus Act of 1878 (18 U.S.C. §1385) was written to ensure that this practice would come to an end.[1]

Though the act codified an American tradition of separating military from civilian affairs, Congress has occasionally authorized the President to deploy military force to enforce, or assist in the enforcement, of various laws. For example, Congress has vested the Coast Guard, a federal armed force, with a broad range of law enforcement responsibilities. Congress has also passed statutes enabling the employment of military force in law enforcement support under specific circumstances, such as permitting the President to call out the armed forces in times of insurrection and domestic violence,[2] or authorizing the armed forces to share information and equipment with civilian law enforcement agencies.[3]

One important example of congressional direction in the use of the armed forces to support law enforcement was seen in the enactment of the National Defense Authorization Act, Fiscal Year 1989.[4] Title XI of the act tasked the Department of Defense (DOD) to assume a prominent role in detecting and monitoring illegal drug production and trafficking. DOD became "the single lead agency of the Federal Government for the detection and monitoring of aerial and maritime transit of illegal drugs into the United States," and the integrator of an effective system of command, control, communications, and intelligence assets dedicated to drug interdiction.[5] The act also placed Coast Guard law enforcement detachments aboard "every appropriate surface naval vessel at sea in a drug-interdiction area" and made "available any equipment (including associated supplies or spare parts), base facility, or research facility of the Department of Defense to any Federal, State or local law enforcement official for law enforcement purposes."[6]

---

[1] *Posse comitatus* refers to the customary English authority of a sheriff to summon the population of his county to his assistance to, for example, keep the peace or arrest felons. The act forbids the willful use of any part of the Army (later expanded to include the Air Force) as a posse comitatus or otherwise to execute the laws.

[2] See 10 U.S.C. §§331-335.

[3] See 10 U.S.C. §§371-382. For more information regarding the background and scope of the Posse Comitatus Act, see CRS Report R42659, *The Posse Comitatus Act and Related Matters: The Use of the Military to Execute Civilian Law*, by Charles Doyle and Jennifer K. Elsea.

[4] Act of September 29, 1988, P.L. 100-456, 102 Stat. 1918.

[5] Ibid., Section 1102 and Section 1103.

[6] Ibid., Section 1104.

Finally, it authorized additional DOD funding to the National Guard for drug interdiction and enforcement operations.[7]

The following year, in the National Defense Authorization Act for Fiscal Years 1990 and 1991, Congress created a pathway for DOD to directly transfer to federal and state agencies equipment (so-called "personal property") that was excess to the needs of the department and suitable for use in counter-drug activities.[8] Under Section 1208, the Secretary of Defense could transfer defense equipment, including small arms and ammunition, from existing defense stocks without cost to the receiving agency. In transferring such property, the Secretary of Defense was required to consult with the Attorney General and the Director of National Drug Control Policy (the federal government's so-called "drug czar").[9] The act included a sunset provision that would have terminated this authority on September 30, 1992. This termination date was extended to September 30, 1997 by the enactment of Section 1044 of the National Defense Authorization Act for Fiscal Year 1993.[10]

The 1033 Program

As the revised termination date approached, the 104th Congress considered making its authority permanent. The House version of the National Defense Authorization Act for Fiscal Year 1997 contained language (H.R. 3230, Section 103) that would have expanded eligibility for property transfers to all law enforcement while retaining a priority for counter-narcotics activities. The Senate's amendment of the bill contained no similar provision. In conference, the Senate receded, but with an amendment that extended priority in property transfer to both counter-narcotics and counter-terrorism activity. The amendment also ensured that DOD would incur no cost beyond management of the program in transferring this excess equipment to these law enforcement agencies. The language was enacted as Section 1033 and is codified under Title 10, Section 2576a, of the United States Code (10 U.S.C. §2576a).[11]

Materials Offered to Law Enforcement Agencies through the 1033 Program

The program is administered by the Law Enforcement Support Office (LESO) of the Defense Logistics Agency (DLA), located at DLA Disposition Services Headquarters in Battle Creek, Michigan. Though participating agencies initiate requests for material, the Defense Logistics Agency (DLA) retains the final authority to determine the type, quantity, and location of excess military property suitable for transfer and use in law enforcement activities.

[7] Ibid., Section 1105.

[8] See Section 1208 of Title XII in the National Defense Authorization Act for Fiscal Years 1990 and 1991 (P.L. 101-189, 103 Stat. 1566) at **Appendix A**. Personal property includes any belongings that are not real estate property, buildings, or other fixed infrastructure. The section was codified as 10 U.S.C. 372 note.

[9] The position of Director of National Drug Control Policy had been created by the 100th Congress as part of the 1988 omnibus drug bill, the Anti-Drug Abuse Act of 1988 (H.R. 5210, P.L. 100-690), and President George H.W. Bush appointed William T. Bennett to the position.

[10] National Defense Authorization Act for Fiscal Year 1993 (H.R. 5006, P.L. 102-484).

[11] This was Section 1033(a)(1) in Division A, Title X, Subtitle B of the National Defense Authorization Act for 1997 (P.L. 104-201, 110 Stat. 2639). It was enacted on September 23, 1996.

General categories of equipment offered for transfer include office furniture, household goods (e.g., kitchen equipment), exercise equipment, portable electric generators, tents, and general law enforcement supplies (e.g., handcuffs, riot shields, holsters, binoculars, and digital cameras). Heavy equipment, such as cranes, and various types of land vehicles are available. Watercraft, aircraft, and weapons are also eligible for transfer. Miscellaneous other property includes tool kits, first aid kits, blankets and bedding, lawn maintenance supplies, combat boots, and office equipment (computers, printers, fax machines, etc.).

Program Participants

Law enforcement agencies wishing to take part in the 1033 Program apply to the LESO through their state's 1033 Program coordinator (see below). Once their participation has been approved by the state coordinator and the LESO, the law enforcement agencies appoint officials to visit their local DLA Disposition Services Site, where they screen property and place requests for specific items. The forms are then forwarded to the state coordinator for review; once approved, the LESO makes the final determination of whether or not the property will be transferred. Law enforcement agencies that receive approval for property transfers must cover all transportation costs.

According to the LESO, 11,000 law enforcement agencies are registered nationwide and 8,000 are currently using property provided through the program.[12]

Material Accountability

Each state participating in the program must set up a business relationship with DLA through the execution of a Memorandum of Agreement (MOA). Each participating state's governor is required to appoint a state coordinator to ensure that the program is used correctly by the participating law enforcement agencies. The state coordinators are expected to keep property accountability records, investigate any alleged misuse of property, and, in certain cases, report violations of the MOA to DLA. The LESO may suspend the participation of a state that cannot properly account for the property entrusted to it, and state coordinators may suspend the participation of any law enforcement agency thought to abuse the program. The chief of police or equivalent senior official of the receiving law enforcement organization is held responsible for all 1033 Program controlled property.

Additionally, DLA has a compliance review program. The program's objective is to have the Law Enforcement Support program staff visit each state coordinator and assist him or her in ensuring that property accountability records are properly maintained, minimizing the potential for fraud, waste and abuse.

Some of the equipment offered to law enforcement through the program, such as weapons or tactical vehicles, possesses significant military capabilities. By law, these items cannot be released to the general public and ownership is never transferred to law enforcement agencies—rather, they are considered to be on loan. This equipment

[12] See DLA Disposition Services website. The LESO defines a law enforcement agency as "a government agency whose primary function is the enforcement of applicable federal, state and local laws and whose compensated law enforcement officers have the powers of arrest and apprehension."

is closely tracked by both the LESO and the relevant state coordinator and it must be returned to a DLA Disposition Services Site when no longer needed for law enforcement purposes.

Property not considered to be uniquely military, such as office equipment or first aid kits, is considered controlled property for the first year that it is held by the agency and must be accounted for in the same manner as all other 1033 Program property. At the end of the year, title is transferred to the law enforcement agency and the property is removed from the audited inventory.

Congressional Reporting Requirements

The statute does not require any regular reports to Congress on the 1033 Program.

Additional Information Resources

More information regarding the 1033 Program is available through the LESO website (http://www.dispositionservices.dla.mil/leso/pages/default.aspx). A number of states maintain their own law enforcement support offices that post program information tailored to their own jurisdictions (e.g., Ohio's Law Enforcement Support Office at http://ohioleso.ohio.gov/).

Appendix A
Text of Section 1208 of the National Defense Authorization Act for 1990 (P.L. 101-189)

SEC. 1208. TRANSFER OF EXCESS PERSONAL PROPERTY

(a) TRANSFER AUTHORIZED—(1) Notwithstanding any other provision of law and subject to subsection (b), the Secretary of Defense may transfer to Federal and State agencies personal property of the Department of Defense, including small arms and ammunition, that the Secretary determines is—

(A) suitable for use by such agencies in counter-drug activities; and

(B) excess to the needs of the Department of Defense.

(2) Personal property transferred under this section may be transferred without cost to the recipient agency.

(3) The Secretary shall carry out this section in consultation with the Attorney General and the Director of National Drug Control Policy.

(b) CONDITIONS FOR TRANSFER- The Secretary may transfer personal property under this section only if—

(1) the property is drawn from existing stocks of the Department of Defense; and

(2) the transfer is made without the expenditure of any funds available to the Department of Defense for the procurement of defense equipment.

(c) APPLICATION—The authority of the Secretary to transfer personal property under this section shall expire on September 30, 1992.

Appendix B
Text of 10 U.S.C. §2576a, "Excess Personal Property: Sale or Donation For Law Enforcement Activities"

§2576a. Excess personal property: sale or donation for law enforcement activities

(a) Transfer authorized.

(1) Notwithstanding any other provision of law and subject to subsection (b), the Secretary of Defense may transfer to Federal and State agencies personal property of the Department of Defense, including small arms and ammunition, that the Secretary determines is—

(A) suitable for use by the agencies in law enforcement activities, including counter-drug and counter-terrorism activities; and

(B) excess to the needs of the Department of Defense.

(2) The Secretary shall carry out this section in consultation with the Attorney General and the Director of National Drug Control Policy.

(b) Conditions for transfer. The Secretary of Defense may transfer personal property under this section only if—

(1) the property is drawn from existing stocks of the Department of Defense;

(2) the recipient accepts the property on an as-is, where-is basis;

(3) the transfer is made without the expenditure of any funds available to the Department of Defense for the procurement of defense equipment; and

(4) all costs incurred subsequent to the transfer of the property are borne or reimbursed by the recipient.

(c) Consideration. Subject to subsection (b)(4), the Secretary may transfer personal property under this section without charge to the recipient agency.

(d) Preference for certain transfers. In considering applications for the transfer of personal property under this section, the Secretary shall give a preference to those applications indicating that the transferred property will be used in the counter-drug or counter-terrorism activities of the recipient agency.[13]

Author Contact Information

Daniel H. Else
Specialist in National Defense
delse@crs.loc.gov, 7-4996

[13] This section was added by the Act of September 23, 1996, P.L. 104-201, Division A, Title X, Subtitle B, §1033(a)(1), 110 Stat. 2639.

DOCUMENT NO. 13

THE "MILITARIZATION" OF LAW ENFORCEMENT AND THE DEPARTMENT OF DEFENSE'S "1033 PROGRAM"

CRS Insights

Nathan James, Analyst in Crime Policy (njames@crs.loc.gov, 7-0264)

Daniel H. Else, Specialist in National Defense (delse@crs.loc.gov, 7-4996)

December 2, 2014 (IN10138)

August 2014 clashes between police and protesters in Ferguson, MO, sparked a national conversation about the "militarization" of law enforcement and the expanding role of Special Weapons and Tactics (SWAT) teams. Both the House and the Senate held hearings on what role the Department of Defense's (DOD) "1033 Program" might play in the militarization of law enforcement.

Militarization of Law Enforcement

SWAT teams first appeared in the later part of the 1960s as a way to respond to extraordinary cases that could not be effectively managed by regular law enforcement personnel. The tactics employed by SWAT teams are designed to protect the safety of officers, the public, victims, and offenders.

The number of SWAT teams has proliferated since they were founded in the 1960s. By the late 1990s, about 89% of police departments in the United States serving jurisdictions of 50,000 or more people, and 80% of departments serving jurisdictions of 25-50,000 people reported having a SWAT team. The growth in the number of SWAT teams in small jurisdictions has raised questions about whether they have the resources necessary to properly train team members.

Data show that SWAT teams are being deployed more frequently. There was a reported 1,400% increase in the total number of SWAT deployments between 1980 and 2000. There are an estimated 45,000 SWAT deployments each year. There is also concern that SWAT teams are experiencing "mission creep." SWAT teams were originally created to respond to extraordinary violent or dangerous situations, such as hostage situations, active shooters, or barricaded suspects. However, data show that now nearly 80% of SWAT deployments are for proactive drug raids or to execute search warrants. In addition, SWAT teams are increasingly used to conduct routine patrol work in crime "hot spots."

A recently released report by the American Civil Liberties Union (ACLU) argues the aggressive tactics used by SWAT teams can exacerbate, rather than diminish, the risk of a violent confrontation. In addition, the ACLU noted that what constitutes a "high risk" situation, thus warranting the use of a SWAT team, is based on the subjective belief of the officers involved. The ACLU also argues that the aggressive techniques used by SWAT teams during routine investigations can have a negative effect on public confidence in law enforcement.

Two scholars argue that the "war on drugs" and the "war on terror" have given rise to the militarization of police by providing a crisis in which law enforcement could expand its size, scope, and power; increasing demands from the public for the government to "do something" about the crisis; and facilitating interactions between the military and law enforcement as they conducted joint operations in the "wars." Technological improvements have lowered the cost for law enforcement to adopt military technology. Technology that was once exclusively used by the military—such as facial recognition systems, thermal imaging, and satellite monitoring—can now be used by law enforcement.

The 1033 Program

The "1033 Program" was created by Congress in the National Defense Authorization Act for 1997 (P.L. 104-201) and is codified in 10 U.S.C. §2576a. It authorizes the Secretary of Defense to provide material support to authorized federal and state law enforcement agencies by transferring articles suitable for counter-drug and counter-terrorism activities. These are drawn from Department of Defense (DOD) stocks deemed excess to military needs.

It was preceded by a 1990 statute, Section 1208 of the National Defense Authorization Act for 1990 and 1991 (P.L. 101-189), that temporarily authorized transfers of defense equipment to law enforcement agencies for counter-drug enforcement use. The 1997 act codified it and included counter-terrorism activities.

The current statute requires that the Secretary of Defense consult with the Attorney General and the Director of National Drug Control Policy in carrying out its provisions. It allows the Secretary to transfer property only if (1) it is drawn from existing DOD stocks, (2) the receiving agency accepts the material "as-is, where-is," (3) the transfer is made without expending DOD procurement funds, and (4) all subsequent costs are borne by the receiver. Nevertheless, the Secretary may transfer the property without charge. Section 1072 of the House's Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (H.R. 4435) would further expand the program to border security enforcement and require the Secretary of Defense to consult with the Secretary of Homeland Security.

The statute specifies that preference will be given to applications indicating that the material will be used in counter-drug or counter-terrorism activities. Section 1085 of H.R. 4435 would expand that preference to the strengthening of U.S.-Mexico border security.

The Law Enforcement Support Office (LESO) of the Defense Logistics Agency (DLA) administers the program. To participate, each state or territory must execute a

Memorandum of Agreement (MOA) with DLA, and the governor must appoint a state coordinator. The coordinator keeps property records, investigates alleged property misuse, and reports MOA violations to DLA. The senior official of the receiving law enforcement organization is responsible for all 1033 Program controlled property. Property requiring demilitarization must be returned to DLA when no longer needed.

State agencies wishing to take part apply to LESO through their state coordinator. Once accepted, these agencies appoint officials to visit a DLA Disposition Services Site and screen available property, placing requests through their state coordinators. LESO has final approval authority over individual transfers.

Material offered by LESO includes office furniture, household goods (e.g., kitchen equipment), exercise equipment, portable electric generators, tents, and general law enforcement supplies (e.g., handcuffs, riot shields, holsters, binoculars, and digital cameras). Heavy equipment, such as cranes, and various types of land vehicles are also available. Watercraft, aircraft, and weapons are eligible. Other property includes tool kits, first aid kits, blankets and bedding, lawn maintenance supplies, combat boots, and office equipment (computers, printers, fax machines, etc.). According to LESO, more than 8,000 agencies participate and have received more than $5.1 billion in property since the program's inception.

SUBJECT INDEX

Afghanistan

Hybrid warfare in, 151, 162, 178

Arms Proliferation

Office of Missile, Biological, and Chemical Nonproliferation in Bureau of International Security and Nonproliferation, 297–298
State Department reporting delays
  comments from Department of State, 299–302
  requirements under INKSNA, 288–289
  time required to complete report, 290–292
  time required to impose INKSNA sanctions, 292–294

Asymmetric Warfare

Defined, 165
See also Hybrid Warfare

China

Aggression and assertiveness, new forms of, 11, 18
Multipolar situation among major world powers, 8, 9
Submarine fleet, 19
See also Post-2013 Shift in International Security Environment

Compound Warfare

Defined, 63, 96
See also Hybrid Warfare

Congressional Research Service (CRS) Reports

"1033 Program," Department of Defense support to law enforcement (CRS Report No. R43701), 361–369
Cyber operations in DOD policy and plans (CRS Report No. R43848), 203–275
Cyberwarfare and cyberterrorism in brief (CRS Report No. R43955), 263–275
Post-2013 shift in international security environment (CRS Report No. R43838), 5–45

Cyber Security

Generally, 203–275
Actors and attribution, 210–211
Advanced persistent threats, 211
Attribution issues, 211
Authorizing and oversight committees, 232
Automated Defense Systems, 208–209
Botnets, 207
Case studies, 212–217
Civil support by DOD, 224, 353, 355, 359
Comprehensive National Cybersecurity Initiative, 222
Consensus-building activities, 226
Council of Europe Convention on Cybercrime, 227, 270
Countermeasures, international law on, 228
Critical infrastructure cybersecurity, 209–210, 223
CRS Report R43848, 203–235
Current legislation, 232–233
Cyber Command Mission and Force Structure, 217–218

Cyber Security (*Cont*)

Cyber weapons, 206–209
Cyberterrorism, explained, 272–273
Cyberwarfare, explained, 267–268
Defense instruments, 229
Department of Defense policy, 203–235
  actors and attribution, 210–211
  advanced persistent threats, 211
  attribution issues, 211
  authorizing and oversight committees, 232
  case studies, 212–217
  civil authorities, defense support for, 224
  consensus-building activities, 226
  critical infrastructure and industrial control systems, 209–210
  critical infrastructure cybersecurity, 223
  current legislation, 232–233
  Cyber Command Mission and Force Structure, 217–218
  cyber weapons, 206–209
  Executive Authorities, 221–224
  Executive Order 13636, 223
  government targets, 209
  hacktivists, 210
  information sharing, 218–219
  interagency and private sector questions, 231
  international authorities, 225–226
  jurisdictional implications, 232
  legislative authorities, 219–221
  military network targets, 209
  nation states, 210
  National Infrastructure Protection Plan, 224
  National Response Framework, 224
  operating environment, 205–206
  organized crime, 210–211
  politically motivated hacktivists, 210
  Presidential Policy Directives, 222–224
  targets, 209–210
  threat environment, 211–212
  unified combatant command, 232
  U.S. Cyber Command, 217–219
  U.S. position on international authorities, 225–226
Distributed denial of service attacks, 207–208
Dubai Summit, 230–231
EINSTEIN, 260
Estonia, cyberattack as siege, 212–213
Executive authorities and directives, 221–224
Federal contractor systems, cyber-based threats, 237–249, 255–256
  events and incidents, 244, 245
  National Cybersecurity Protection System (EINSTEIN), 260
  recent data breaches, 251–262
  recommendations, 247–249
  risks and weaknesses, 240, 257
  sources of threats, 241–242
  types of threats, 242–243
Georgia, cyberattack and invasion, 213–215
Government Accounting Office Reports
  GAO-15-573T, 237–249
  GAO-15-725T, 251–262
Government targets, 209
Hacktivists, 210
Homeland Security Presidential Directive 23, 222
Industrial control systems, 209–210
Information sharing, 218–219
Interagency and private sector questions, 231
International law, 269–272
  international authorities, 225–226
  International Code of Conduct for Information Security, 230
  international instruments bearing on cyberwarfare, 227–231
Iran, cyberattack with kinetic effect, 217
Issues for Congress, 231–233
ITU Dubai Summit, 230–231
Jurisdictional implications, 232
Law of armed conflict/law of war, 228, 269–270
Legislative authorities, 219–221
Military
  military network targets, 209
  offensive cyberspace operations, 273–275
Nation states, 210
National Cybersecurity Protection System (EINSTEIN), 260
National Infrastructure Protection Plan, 224
National Response Framework, 224
National Security Presidential Directive 54, 222
Norm-building, 268–272
North Atlantic Treaty Organization (NATO), 228–229
Operating environment, 205–206
Organized crime, 210–211
OSCE Early Warning Resolution, 230
Politically motivated hacktivists, 210
SCO-Proposed International Code of Conduct for Information Security, 230

Separate cyber force, necessity of, 232
Targets, 209–210
Telecommunications regulations, 229, 271–272
Threat actors, 265–267
Threat environment, 211–212
Timeline of international attacks, 233–235
Unified combatant command, 232
United Nations Resolutions, 227–228, 271
U.S. Cyber Command, 217–219
U.S. federal and contractor systems, cyber-based threats, 237–249, 255–256
  recent data breaches, 251–262
  risks enumerated, 240
U.S. Government Accountability Office reports
  GAO-15-573T, 237–249
U.S. position on international authorities, 225–226

Department of Homeland Security

Civil support, 350, 352
Cyber security, 203, 219, 238, 240, 252, 253, 265

European Union

Council of Europe Convention on Cybercrime, 227, 270
Estonia within, 212, 213
Political warfare, U.S. diplomacy, 171, 176
Post-2013 shift in international security environment, 16–17

Fourth Generation Warfare

Defined, 62, 63, 97
See also Hybrid Warfare

Government Accountability Office (GAO) Reports

Cybersecurity
  data breaches, need for controls across federal agencies, 251–262
  threats to federal and contractor systems (GAO-15-573T), 237–249
DOD action to strengthen support of civil authorities (GAO-15-686T), 349–359

"Gray Zone"

Within current international security environment. *See* Post-2013 Shift in International Security Environment
Explained, *ix*, 100–101
See also Hybrid Warfare

Hybrid Warfare

Generally, 53–157
Archetype for operational approaches to hybrid warfare, 139–140
Combinations in multiple domains, 95–96
Comments from Department of Defense, 157
Competing models of mixed forms of warfare, 95
Compound warfare, 96–97
"Compound warfare," 63
Within current international security environment. *See* Post-2013 Shift in International Security Environment
Dau tranh theory of warfare, 110–114
Definitions, *ix*, 61, 63, 151–153, 155–156, 169
  lack of consensual understanding, 61–68
End state myopia, 142
Fourth generation warfare, 62, 63, 97
Future research, implications for, 85
GAO report, 145–157
Generational theory of modern warfare, 61, 62
Grammar metaphor, 103
Gray spaces, 100–101
Historical analysis, 53–145
Imperatives for operational art in hybrid warfare, 138–139
Implications of hybrid war theory, 83–84
Iraq, 122–137
Israel-Hezbollah War of 2006, 71–77
JSOU (Joint Special Operations University) report, 53–144
Land operations, sufficiency of operational art in, 142–143
Legitimate violence, 143–144
Multiple domains, 95–96
Nature of, 93–101
New ways of explaining hybrid behavior, 68–71
Newness of hybrid threat, 57–85
Objectives, 151–154
Operation Iraqi Freedom, 122–137
Operational approaches, 87–144
Operational art, 101–107
Other types of warfare compared, 151–152
Paradigm shift, 61, 63
Passive interconnection in Iraq, 124–126
Potential outcomes, 84–85
Protraction of conflict, 97

Hybrid Warfare (*Cont*)

Review of existing hybrid warfare thinking and doctrine, 61–68
Shock and dislocation, 140–141
Social pressures, 61
Soviet partisan network of WWII as hybrid organization, 77–82
Statehood, 93–95
Strategic planning, 154
Symmetry, 93–95
Synergistic effects of hybrid principles in action, 82
Synthesis of military theory and historical trends, 83–85
Theoretical evolution of warfare, 61–64
  existing hybrid warfare theory, 97–99
  operational art, 103–105
  theory-practice, 102
Thought processes, 62
Unified land operations, sufficiency of operational art in, 142–143
Unifying thought process, 62
U.S. Army doctrine, threat-based focus, 99–100
U.S. Government Accountability Office report, 145–157
Venn diagram, 127
Vietnam, 107–122
World War II Eastern Front, 77–82
See also Post-2013 Shift in International Security Environment

International Security Environment

Shift in, 5–45
See also Post-2013 Shift in International Security Environment

Iran

INKSNA, curbing weapons of mass destruction proliferation, 281–304

Iraq

Hybrid warfare in
  generally, 91, 92, 122
  Operation Iraqi Freedom, 122–137
  passive interconnection, 124–126

"Lawfare"

As element of hybrid warfare, *ix*

Legislation—Federal

Cyber security, current legislation, 232–233
Post-2013 shift in international security environment, legislative activity in 2015, 21–45

Military—Role of

Civil support by DOD, 349–359
  capability gaps, 357–359
  findings, 350–353
  GAO-15-686T, 349–359
  interagency coordination, 355–357
  needs identification, 357–359
  "whole-of-government" approach, 356
Law enforcement support via "1033 Program," 363–365
  generally, 361–369
  categories of equipment offered for transfer, 364
  CRS Report R43701, 361–369
  equipment and materials offered, 363–364
    accountability, 364–365
    statutory authorization, 365, 366
  "militarization" of law enforcement, 367–369
  National Defense Authorization Act for 1990 (P.L. 101-189), 365
  program participants, 364
  10 U.S.C. §2576a, 366
  tradition of separating military from civilian affairs, 362
Political warfare, SOF support, 159–197
See also Political Warfare, SOF (Special Operations Forces) Support

National Security—Threats to

Change in, 5–25
See also Post-2013 Shift in International Security Environment

North Korea

INKSNA, curbing weapons of mass destruction proliferation, 281–304
Sanctions, 305–344
  activities targeted, tables of, 316, 332

Commerce Department, export controls on items shipped to North Korea, 323–324
financial transactions, 316–318
luxury goods, 311–318
recommendation for executive action, 331
State Department
comments, 342–343
consensus before making final determination, 321–322
Executive Order addressing flexibility and factors hindering process, 318–319
historical sanctions, 322–323
Treasury Department working groups, review of intelligence and other information on potential targets, 320–321
United Nations, 324–330
1718 Committee, oversight by, 325–326
illicit techniques used by North Korea to evade sanctions, 327–328
member states implementation report, 335–341
panel of experts to monitor and facilitate sanctions, 326–327
U.S. interagency process to determine when and whether to impose sanctions, 319–324
executive orders addressing factors hindering process, 318–319
U.S. Government Accountability Office report GAO-15-485, 305–344

Nuclear Nonproliferation

Sanctions on trade with Iran, North Korea, and Syria, 281–304

Political Warfare, SOF (Special Operations Forces) Support

Generally, 159–197
Building partner capacity (BPC), 177–178
Centrality of SOF to political warfare, 191–193
China's unrestricted warfare, 164–165
Cognitive Joint Force Entry (CJFE), 185–186
Cold War and political warfare, 160–161
Computing power, 168–169
Counter-unconventional warfare (C-UW), 180–181
Diplomacy, 171–174, 184–185
Economic aid or coercion, 174–175
Foreign internal defense (FID), 178
Future operating environment, 167–169
Global power diffusion, 167
Groups, identification of, 196–197
Hezbollah, 166–167
Human domain, 186–187, 196–197
Hybrid warfare, defined, 169
Individuals, identification of, 196–197
Information and communications technologies, 168–169
Information and influence activities (IIA), 182–186
Iranian asymmetric warfare, 165–166
Military Information Support Operations (MISO), 185–186
Military problem and components of solution, 169–193
Non-state and semi-state actors, 167–168
Operational capabilities, 193
Populations, identification of, 196–197
Post-Cold War, 161–162
Precepts of political warfare, 189–191
Proactive fashion (Pr-UW), 181–182
Public affairs (PA), 183–184
Regional and global engagement, 192–193
Russia, 162–164
Security sector assistance, 175–178
Security sector reform (SSR), 175–177
Solution concepts and components, 193–197
Statement of problem, 169–170
Traditional unconventional warfare, 180
Unconventional warfare (UW), 178–182
United States Army Special Operations Command, 159–197
Whole-of-government approach, 171–191

Post-2013 Shift in International Security Environment

Generally, 5–45
Aggression and assertiveness, new forms of, 17–18
Authoritarianism, 21st-century forms, 8
China
aggression and assertiveness, new forms of, 11, 18
multipolar situation among major world powers, 8, 9
submarine fleet, 19

Post-2013 Shift in International Security Environment (*Cont*)

Cold War era
  compared, 11–12
  explained, 8
European Reassurance Initiative (ERI), 44
  funding and support, 26–27
Grand strategy and geopolitics, 12–13
Hegemon in Eurasia, 13
Issues for Congress, 20–21
Legislative activity in 2015, 21–45
National Defense Authorization Act, 21–43
Nuclear weapons and nuclear deterrence, 18–19
Post-Cold War era
  compared, 11–12
  explained, 8
  reassessment of U.S. defense during previous shift, 13–15
Russia
  aggression and assertiveness, 11, 17
  multipolar situation among major world powers, 8, 9
  nuclear weapon power, 18
  submarine fleet, 19
  systems and components for U.S. military systems, 20
  unconventional warfare, 24–25
Submarines and antisubmarine warfare, 19–20
U.S. and NATO military capabilities in Europe, 16–17
U.S. Defense, potential or emerging implications for, 15–20

Russian Federation

Aggression and assertiveness, 11, 17
Multipolar situation among major world powers, 8, 9
Nuclear weapon power, 18
Submarine fleet, 19
Systems and components for U.S. military systems, 20
Unconventional warfare, 24–25
See also Post-2013 Shift in International Security Environment

Syria

INKSNA, curbing weapons of mass destruction proliferation, 281–304

United Nations—General Assembly Resolutions

Cyber security, 227–228

Unrestricted Warfare

Defined, 95
See also Hybrid Warfare

Weapons of Mass Destruction

Office of Missile, Biological, and Chemical Nonproliferation in Bureau of International Security and Nonproliferation, 297–298
Reporting delays
  comments from Department of State, 299–302
  requirements under INKSNA, 288–289
  time required to complete report, 290–292
  time required to impose INKSNA sanctions, 292–294