

THE DECISION TO ATTACK

Military and Intelligence Cyber Decision-Making

AARON FRANKLIN BRANTLY

THE DECISION TO ATTACK

This page intentionally left blank



STUDIES IN SECURITY
AND INTERNATIONAL AFFAIRS

SERIES EDITORS

William W. Keller
Professor of International Affairs,
Center for International Trade and Security,
University of Georgia

Scott A. Jones
Director of Export Control Programs,
Center for International Trade and Security,
University of Georgia

SERIES ADVISORY BOARD

Pauline H. Baker
The Fund for Peace

Eliot Cohen
Paul H. Nitze School of Advanced International Studies, Johns Hopkins University

Eric Einhorn
Center for Public Policy and Administration, University of Massachusetts, Amherst

John J. Hamre
The Center for Strategic and International Studies

Josef Joffe
Hoover Institution, Institute for International Studies, Stanford University

Lawrence J. Korb
Center for American Progress

William J. Long
Sam Nunn School of International Affairs, Georgia Institute of Technology

Jessica Tuchman Mathews
Carnegie Endowment for International Peace

Scott D. Sagan
Center for International Security and Cooperation, Stanford University

Lawrence Scheinman
Monterey Institute of International Studies, CNS-WDC

David Shambaugh
The Elliott School of International Affairs, George Washington University

Jessica Stern
FXB Center, Harvard School of Public Health

This page intentionally left blank

The Decision to Attack

Military and Intelligence Cyber Decision-Making

Aaron Franklin Brantly

The University of Georgia Press
Athens

© 2016 by the University of Georgia Press
Athens, Georgia 30602
www.ugapress.org
All rights reserved
Designed by
Set in 10/13 Minion Pro by Graphic Composition, Inc., Bogart, Georgia
Printed and bound by
The paper in this book meets the guidelines for
permanence and durability of the Committee on
Production Guidelines for Book Longevity of the
Council on Library Resources.

Most University of Georgia Press titles are
available from popular e-book vendors.

Printed in the United States of America
20 19 18 17 16 c 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data

Names: Brantly, Aaron Franklin, author.
Title: The decision to attack : military and intelligence cyber decision-making / Aaron Franklin Brantly.
Other titles: Military and intelligence cyber decision-making
Description: Athens, GA : University of Georgia Press, [2016] | Series: Studies in security and international affairs | Includes bibliographical references and index.
Identifiers: LCCN 2015032334 | ISBN 9780820349206 (hbk. : alk. paper) | ISBN 9780820349190 (ebook)
Subjects: LCSH: Cyberspace—Security measures—Government policy—United States. | United States—Military policy—Decision making. | Offensive (Military science)
Classification: LCC U163 .B69 2016 | DDC 355.4/1—dc23 LC record available at http://lccn.loc.gov/2015032334

I dedicate this book to my wife and best friend, Nataliya. She has stood by me and waited for more than five years while I finished my formal academic education and now as I have taken on the challenge of studying Cyber at the United States Military Academy's Army Cyber Institute. She has read, commented on, and reread more of my words than anyone. It is her patient and enduring support that has enabled me to make it as far as I have.

This page intentionally left blank

CONTENTS

List of Illustrations xi

Acknowledgments xiii

List of Abbreviations xv

CHAPTER 1. Introduction to Cyber Decision-Making 1

CHAPTER 2. The Key Concepts of Cyber 25

CHAPTER 3. The Motivation and Utility for Covert Action 43

CHAPTER 4. Digital Power 63

CHAPTER 5. Anonymity and Attribution in Cyberspace 79

CHAPTER 6. Cyber and Conventional Operations: The Dynamics of Conflict 90

CHAPTER 7. Defining the Role of Intelligence in Cyberspace 101

CHAPTER 8. How Actors Decide to Use Cyber—a Rational Choice Approach 125

CHAPTER 9. Cognitive Processes and Decision-Making in Cyberspace 150

CHAPTER 10. Finding Meaning in the Expected Utility of International Cyber Conflict 157

APPENDIX A. Power Score Components and Scores 169

APPENDIX B. Modified Economist Intelligence Unit Component Values 171

APPENDIX C. Affinity Scores 189

Notes 191

Works Cited 203

Index 217

This page intentionally left blank

ILLUSTRATIONS

TABLES

1.1 Examples of Cyber-Controlled Instruments Pertinent to National Security 5

1.2 Presidential Directives, Decisions, and Executive Orders Pertaining to IT and Cyber, 1993–2009 8

1.3 The Cyber Warfare Lexicon 15

4.1 Components of Power 73

4.2 Power Scores by Country (2011) 77

5.1 Probability of Maintaining Anonymity by Attack 86

7.1 Intelligence Collection Methods 104

7.2 Components of Cyber DBA and DBK 112

7.3 Cyber Threat Spectrum 117

8.1 Expected Utilities across Incidents 141

8.2 Results of *t*-Tests of Utilities 145

8.3 T-Tests of Affinity of State Likelihood of Conflict 146

8.4 T-Test of State Affinity in Year Prior to Conflict 147

FIGURES AND CHARTS

1.1 Understanding State Policy Positions 14

2.1 The Modern Structure of National Security 27

2.2 Graphical Representation of Information Diffusion in the New Public Square 29

2.3 Percentage of Individuals Using the Internet (2011) 41

3.1 Fearon's Bargaining Range 47

3.2 Bilateral State Policy Interaction Possibilities 49

3.3 Covert Action Ladder 55

4.1 Percentage of Individuals Using the Internet within Countries in the Sample (2011) 75

6.1 Objective, Scale, and Tools of Conflict 99
7.1 Timeline for Attack Implementation 121
7.2 The Influence of Intelligence on Cyber Operations 122
8.1 State Cyber Power Scores (2011) 139
8.2 Expected Utilities Box Plot 144
8.3 Distribution of Changes in Affinity over Time 146
8.4 Distribution of State Affinities in Year Prior to Hostilities 148

ACKNOWLEDGMENTS

This book would not have been possible without the support and dedication of the diverse cadre of individuals standing behind me and pushing me forward. In particular, I would like to thank Dr. Loch K. Johnson for his constant feedback and assistance in helping me develop the ideas presented in this book. Dr. Johnson has inspired me both as a professor and as a mentor. I would also like to thank Dr. Jeffrey Berejikian, Dr. Han S. Park, Dr. Michael Warner, and Dr. Christopher Bronk, each of whom have given enormous amounts of time to help me with my academic and professional pursuits. Lastly, I would like to thank the team at the United States Army Cyber Institute and the Combating Terrorism Center at the United States Military Academy for providing me the opportunity to engage in research in line with my interests.

The views expressed here are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

This page intentionally left blank

ABBREVIATIONS

CENTCOM	Central Command
CA	cyber attack
CD	cyber defense
CE	cyber exploitation
CERT	computer emergency response team
CINC	Composite Index of National Capabilities
CLT	construal level theory
CO	cyber operations
COW	Correlates of War project
CSIS	Center for Strategic and International Studies
C2W	command and control warfare
CWC	cyber warfare capability
CWS	cyber weapons system
CYBERINT	cyber intelligence
DBA	dominant battlespace awareness
DBK	dominant battlespace knowledge
DCO	defensive cyber operations
DCO-IDM	defensive cyber operations—internal defense measures
DCO-RA	defensive cyber operations—response actions
DDoS	distributed denial of service
DoD	Department of Defense
DoDIN Ops	Department of Defense information networks operations
DoS	denial of service
EIU	Economist intelligence unit
ESC	economic and social context
GEOINT	Geospatial intelligence
HUMINT	human intelligence
IA	industrial application
IAEA	International Atomic Energy Agency
ICE-A	intelligence on the cyber environment of the adversary
ICE-D	intelligence on the cyber environment for defense
ICS	industrial control systems
ICT	information communications technology
INTs	intelligence collection categories

IPB	intelligence preparation of the battlefield
ISP	Internet service provider
LRF	legal and regulatory frameworks
MASINT	measurement and signatures intelligence
MBA	military budget allocation
MUD	military unit designation
NDV	national digital vulnerability
NSA	National Security Agency
OCOs	offensive cyber operations
OSINT	open source intelligence
PII	personally identifiable information
PLC	programmable logic controller
REDEU	rank-dependent expected utility
SAM	surface-to-air missile
SCADA	supervisory control and data acquisition
SIGINT	signals intelligence
TCP/IP	Transmission Control Protocol/Internet Protocol
TI	technological infrastructure
TSC	threat spectrum capabilities
TTPs	tactics, techniques, and procedures
USCYBERCOM	United States Cyber Command

THE DECISION TO ATTACK

This page intentionally left blank

CHAPTER 1

Introduction to Cyber Decision-Making

THE DEBATE OVER the importance of cyberspace has resulted in the consideration of a new domain of operation vital to national security. States find themselves in an increasingly interconnected world with a diverse threat spectrum and little understanding of how decisions are made within this amorphous domain. A great deal of ink has been spilled trying to define what cyberspace is, yet defining the domain itself is only partially helpful in trying to understand why states do what they do within the domain. This book examines whether states rationally decide to engage in offensive cyber operations against other states. To answer this question, many aspects of national security are scrutinized to determine what relevant attributes are associated with a rational decision to engage in offensive cyber operations. These attributes are contextualized into a systemic decision-making model predicated on rational expectations for utility. The book provides a framework within which to understand state decisions in cyberspace. The goals of this book are to facilitate a rigorous understanding of basic decision-making for offensive behavior within cyberspaces and to provide policy-makers with a foundation for constructing sound policies to address new and complex issues.

Is it really necessary to create an entirely new decision-making model for the cyber domain? The following chapters provide dozens of examples that establish how the cyber domain is distinct from more conventional domains of military and intelligence. What differentiates cyberspace from these other domains are four primary attributes. First, the cyber domain is man-made. Second, military capabilities across the other domains are managed through the cyber domain. Third, military and civilian aspects of the cyber domain are often intertwined and difficult to differentiate. Fourth, attribution within cyberspace is often difficult to assign. These attributes combine to create a novel domain of interaction necessitating a nuanced and rigorous decision-making model predicated on existing models for conventional state behavior.

To understand a decision it is necessary to establish an ontological foundation rooted in a fundamental nature of being. Decisions in cyberspace for the purposes of this book are rooted in a rational choice decision-making model based on Bruce Bueno de Mesquita's development of an expected utility theory

of international conflict in which he maps out values of characteristics associated with the instigation of international conflict. The major argument contained within the subsequent chapters assumes that man and, by extension, states are rational entities. Hence the argument builds a rational actor model predicated on the assumption that nation-state cyber actors seek to achieve positive policy outcomes through the engagement of offensive operations with cyber weapons. Although the argument is rooted in a rational choice argument, it does digress in chapter 9 to present alternative cognitive approaches that might extend the debate on decisions relevant to cyberspace.

This introductory chapter has two main tasks: to outline what cyber is and why it is important, providing the reader with a framework within which to understand the topic for discussion; and to examine what conventional decision-making models have done and why they fail to account for the uniqueness of the cyber domain.

WHAT IS CYBERSPACE AND WHY IS IT IMPORTANT?

Cyberspace has a rich, albeit short, history. Begun as a project of the Advanced Research Project's Agency in the 1960s, it was designed to solve command and control issues arising out of the U.S.-Soviet arms race. Cyberspace is often traced to two creators, Vinton Cerf and Bob Kahn;[1] however, the story of the evolution of this new domain is far more complex. Although these two pioneers in networking and TCP/IP (Transmission Control Protocol/Internet Protocol) established the protocols of the modern information renaissance, the roots of cyberspace are more accurately placed with Donald Davies, a researcher with Britain's National Physical Laboratory, and Paul Baran, a Polish émigré and researcher at RAND.[2] The process of development from the early computing machines to something now recognizable as the modern Internet was a combined military and civilian effort fraught with bureaucracy, passion, and unexpected benefits along the way.[3] What defines the Internet is not its intrinsic physical characteristics in the way that land is defined by its terrestrial nature, sea by vast amounts of water, and air by its fluid properties. Instead, the Internet is defined by the linking of computers and the creation of a virtual space that would evolve into a popular science fiction term coined in the 1980s as "Cyberspace."[4]

Computers, the basic unit of the cyber domain, run on simple coding forms constructed of 1s and 0s indicating the on and off of electrical impulses. Long chains of electrical impulses form commands. These commands are written in long blocks called code. Historically, coding was time consuming and difficult, often done on punch cards fed into machines. The difficulty of coding eventually gave rise to programming languages. These languages provided a simplified means of writing code. Coding languages are written in logical if-then

statements that interact with one another. These statements are then built on top of one another into ever more complicated combinations forming firmware and software.[5]

Conceptually, firmware and software are directions or recipes for action that all return back to the distribution of electrical impulses within hardware.[6] These impulses are incredibly fast and provide end users with a virtually seamless functional experience. However, without these impulses and the commands and the logical statements defining the commands, the computer, the fundamental particle of the cyber domain, is nothing more than a box of plastic and metal. The device is then similar to a rock: it cannot be given a verbal command or told what to do or have any existential meaning beyond its atomic structure, geoposition, mass, and volume.

The value of the cyber domain lies in its ability to create a virtual world from trillions of commands hopscotching around the world and interacting with one another in logically defined environments and in the ability of commands within digital environments to control devices. A computer is incapable of irrationality. Giving a computer competing logical statements can test the rationality of a computer. Most computer users have had this happen to them. Their computer freezes, or the mouse icon spins. The logical routine is stuck and cannot proceed.

The value of cyberspace is a reflection of connections to the systems of logic and is contained in its ability to store, interact, connect, and control. The power and danger of cyberspace is the relationship that information has with the world around it and the way in which users in a social environment access and manipulate or understand that information. Computers monitor the emergency systems of a nuclear power plant and alert operators and other systems connected to it whether core temperature is too high or too low. Information communications technologies known as industrial control systems (ICS) facilitate the safe and efficient operation of these plants. Similarly, computers often monitor where trains are within a subway system to prevent them from getting too close to one another or to alert them that a section of track is not functioning. When this code fails, as was the case in the Metro collision in Washington, D.C., in 2009, digital failure yields real-world pain.[7] Cyberspace is valuable because it connects—and controls and interacts with—aspects of our everyday lives. It is the interaction and the increasing dependence on cyberspace that influence its value.

Increasing connections cause the cyber domain to expand and increase its value. Whereas the value of land increases as it becomes scarcer or the content of that land is found to have items contained within it of value to the market, the value of cyberspace increases in a dynamic relationship with its connections. The growth in value is neither linear nor exponential; however, the value is inherent and can be easily understood.

Our lives, our hopes, and our existence in modern society are directly tied to the cyber world. We depend on magnetic strips on credit cards to feed and clothe us. We tote mobile lifelines, send e-mails, receive phone calls, and conduct commerce on electronic devices. Our bank accounts are numbers stored in computer databases, and the value of our life savings can be wiped away with a stroke of a keyboard. But beyond these modern inventions we are dependent on the electromagnetic spectrum to manage our power grids and the ordering systems that ensure our gas stations have fuel and our grocery stores have food. We don't have to plug ourselves into the matrix; we already live in it.

The domain is remarkably fragile when compared with conventional domains in that a disruption in the connections that link us to the domain can have a profound effect on our lives. It is very difficult to remove people from land without killing them, detaining them, and forcibly moving them. Land is static. People using the land must be moved to deny them access. The same is not true of cyber. To deny an individual access, all that is necessary is to turn off the power, cut the cord, or shut down an Internet service provider (ISP). Anyone who has ever tried to buy groceries during a blackout has found it extremely difficult without being in possession of previously procured hard currency, and even then most stores cannot conduct business without electricity, as their sales and inventory systems are dependent on digital connections. Not only can an individual not withdraw hard currency when the power is down, he or she cannot use a credit card to purchase goods. These connections sustain modern society and undergird the fabric of our everyday lives.

Much as the general public has become increasingly dependent on cyberspace and its increases in communications, efficiency, and general facilitation of activities in modern life, information communications technology has also dramatically altered the landscape of national security and created a revolution in military affairs.[8]

Cyberspace is important and dramatically affects our lives in many ways, but what is cyber? Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz acknowledge more than nineteen different definitions of cyberspace, giving a moving target, difficult to pin down.[9] This book has settled on Dan Kuehl's definition as the most encompassing of various agencies and author positions. Kuehl defines cyberspace as follows:

> A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.[10]

The above definition is formal and difficult to fully digest. So before moving on it is necessary to deconstruct its component parts.

TABLE 1.1 Examples of Cyber-Controlled Instruments Pertinent to National Security

Satellites	Radio transmissions
Drones	GPS
Heads-up displays for pilots	Most modern avionics
Communications technologies	Logistical coordination systems
Intellipedia	Smart projectiles
Electric grids	Power plants
Banks	Stock exchanges

All of the above items in some way make use of cyber for their operation. This table does not distinguish between public and private cyber domains.

Electronics: the branch of physics and technology concerned with the design of circuits using transistors and microchips, and with the behavior and movement of electrons in a semiconductor, conductor, vacuum, or gas.[11]

Electromagnetic Spectrum: the range of wavelengths or frequencies over which electromagnetic radiation extends.[12]

More simply, these two define the physical characteristics of the domain. The operational characteristics of this domain are defined by the creation, storage, modification, and exploitation of data (information). The target of operations or the asset within a domain is information. This information can be used to influence both intradomain operations (for example, how information is displayed or shared on a network) and extradomain operations, manipulating the output of an information process such as how a robot in a car manufacturing plant operates to place pieces together.

What is information? Information is a very broad concept best summarized for cyber as follows:

Information: Computing data as processed, stored, or transmitted by a computer.[13]

This definition hides the value the word itself contains. Data can be programs designed to operate factories, devices, power stations, and much more. But data can also be facts and figures about people, places, and things. Both types of data have value and often can be interoperable. One type is proactive in affecting digital processes; the other is static in that its value is determined by the user or consumer.

Despite definitions of the component parts of the domain, it remains difficult to fully understand what the domain constitutes. Table 1.1 is a list of a small sampling of those aspects of national security connected to cyberspace.

Yet as robust as Kuehl's definition is, it is not the current definition used by United States Cyber Command (USCYBERCOM). USCYBERCOM defines cyberspace as "a global domain within the information environment consist-

ing of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers."[14] The USCYBERCOM definition is narrower than Kuehl's definition yet does not invalidate it. Because every nation around the world views cyberspace differently, it is best to leverage the broadest possible, yet still technically accurate, definition. It is for this reason that all references to cyberspace leverage Kuehl's definition over the official U.S. government one.

Cyber is amorphous and evolving. Tangible boundaries between countries within cyber are difficult to identify and easy to overcome in many instances.[15] While the conventional domains of land, sea, and air are bounded, the cyber domain increases in size and value with every new connection and every advance in computing power. Although cyberspace has been defined above, its importance to everyday life and national security is integral to understanding it from a military and intelligence perspective.

For military commanders and their soldiers on the battlefield, communication always has been important. Communications technologies have evolved significantly since the use of tools such as the semaphore, a system of flags that could send up to 196 different signals developed more than two hundred years ago.[16] The digital revolution for information communications technologies can be traced back to the Crimean War and the extension of European telegraph lines.[17] The Crimean War was the first conflict in which policy-makers at home could quickly and efficiently receive and transmit information on operations in the field hundreds, if not thousands, of miles away. The 1899 invention of the wireless further advanced the information revolution.[18] Each of these advances played a dramatic role not only in the conduct of warfare from an organizational perspective but also from a policy perspective. Battlefield information could be transmitted back to populations and greatly affect popular perceptions of conflict.

These early technologies were limited and often had drawbacks. Telegraph lines could be cut, preventing critical information from reaching its destination, or worse, telegraph lines could be tapped and provide an enemy with information on troop movements, positions, logistics, and strategy. Radios contained many of the same problems of their telegraph cousins. The signals could be intercepted and read. Worse still for aviators or to the benefit of their targets, information technology had not caught up with the needs of aviators. Radio transmissions during World War I from Luftwaffe aircraft and zeppelins could provide reliably accurate time and target information and allow for defensive actions over Great Britain.[19] Later in World War II the use of radar allowed for early warning of incoming aircraft with a greater degree of accuracy than radio triangulation, but because it was a new technology and its operators were rela-

tively inexperienced, the information it provided was critically ignored or misinterpreted in the bombing of Pearl Harbor.[20]

Each new development in information communication technology has advanced the conduct of modern warfare from both a military strategic and tactical, as well as an intelligence collection and operations perspective. Information communications technology is not new. It has, as the two previous paragraphs illustrate, been used for more than a century. Information transmission has evolved since its infancy, gaining in prominence in multiple ways. The importance of information has grown significantly with the invention of computers.

Computers have been around since just prior to World War II. Early computers were massive, were difficult to use, and had limited functionality. Enormous progress was made on computers throughout the postwar period. The most dramatic stride in computing occurred with the invention of ARPANET by the Defense Advanced Research Project Agency on October 29, 1969.[21] Whereas previously computers were independently functioning machines, ARPANET linked these machines, enabling them to communicate with one another. The dramatic strides of ARPANET and progress on computer processing power were of immense value and influenced modern society in everything from commerce and banking to national security and defense. The next great leap forward in the information revolution occurred with the development of the World Wide Web.

John Arquilla and David Ronfeldt early on contended that information has risen from a tool in support of strategic and tactical advantage to a "fourth dimension of national power."[22] This view, however, is somewhat ignorant of the role of information in the conduct of state and international relations over time and places a newness of emphasis on an aspect of national power that has been of significance for millennia. Information has been a vital aspect of national and international political power since before Sun Tzu in the sixth century B.C. and Kautilya in 350 B.C. [23] Joseph Nye, widely known for his writings on power and its relationship to states in international relations, finds that cyberspace is part of an information revolution.[24] The value of information has always been inherent in the development of power; however, the tools to quickly access information are quite modern.

Cyberspace is a domain through which information transmissions have flourished. While the advent of the Gutenberg press spread the written word and enhanced information transmission, information was still limited to those who could afford it. For centuries information was kept mainly by the few, but in the last thirty years the diffusion of information has increased in pace. In the 1970s and even in the 1980s a scholar had to go to a library to find articles written by his or her peers; now the library quite literally can go where the author is. The July 2011 "Department of Defense Strategy for Operating in Cyberspace" makes note that in the last ten years alone the number of Internet users has risen

TABLE 1.2 Presidential Directives, Decisions, and Executive Orders Pertaining to IT and Cyber, 1993–2009

Directive	Title	Date
PDD/NSC 3	Public Encryption Management	15 Apr. 1993
PRD/NSC 27	Advanced Telecommunications and Encryption	16 Apr. 1993
PRD/NSC 48	International Market for Software Products Containing Encryption	1994
PRD/NSC ??	Information Assurance	14 Mar. 1996
PDD/NSC ??	Encryption Export Policy	15 Nov. 1996
PDD/NEC ?	Electronic Commerce	1 July 1997
PDD/NSC 63	Critical Infrastructure Protection	22 May 1998
PDD/NSC 66	Encryption Policy	16 Nov. 1998
PDD/NEC ?	Further Work on Electronic Commerce	30 Nov. 1998
PDD/NSC 68	U.S. International Information Policy	30 Apr. 1999
NPSD 16	To Develop Guidelines for Offensive Cyber Warfare	July 2002
HSPD	Critical Infrastructure Identification, Prioritization, and Protection	17 Dec. 2003
NSPD 38	National Strategy to Secure Cyberspace	2004
NSPD 54	Cyber Security and Monitoring	8 Jan. 2008
HSPD 23	Cyber Security and Monitoring	8 Jan. 2008
PPD 20	U.S. Cyber Operations Policy	16 Oct. 2012
PPD 21	Critical Infrastructure Security and Resilience	12 Feb. 2013
EO 13636	Improving Critical Infrastructure Cybersecurity	12 Feb. 2013

Source: "Presidential Directives and Executive Orders."

? represents directive numbers that are unavailable.

from approximately 360 million to more than 2 billion.[25] Google announced in 2010 that it had scanned over 12 million books and later that same year established the goal of scanning the remaining known 118 million volumes by the end of the next decade.[26] These efforts effectively place the equivalent of the collective knowledge of humanity within a few mouse clicks. Yet, the ability to store information is not the only important aspect of the cyber domain.

There are numerous departmental, congressional committee, and executive reports and analyses on the value of information technology and cyberspace. Table 1.2 highlights the importance of the cyber domain by referencing presidential directives directly relating to information technology and cyberspace. The table provides just a small snapshot of the broader governmental efforts to understand, safeguard, and employ the cyber domain.

Within the large-scale governmental emphasis on the cyber domain, nowhere has the information revolution had more of an impact than on the U.S. Department of Defense. While the information revolution can be traced back well before the rise of the Internet, the clear turning point in the information revolution of military affairs came during the first Gulf War, which is often regarded as the first successful use of command and control warfare (C2W).[27] C2W rendered the majority of Iraqi forces impotent as U.S. forces entered the

country in 1990.[28] Information technology, cyber tools, used in the conduct of this war created a revolution in military affairs (RMA).[29] The evolution of U.S. military dependence has only increased since the first Gulf War. The changes in the information connectedness of war have resulted in a change in the function of command.[30] At present the U.S. military relies on network-centric warfare to conduct its operations around the world, and the U.S. intelligence community relies on multiple cyber tools for collection and dissemination of intelligence.[31]

The value of cyberspace for national security has grown if not exponentially, then close to it over the previous two decades. Beneath the collaboration of the military and intelligence communities is the storage of the country's modern crown jewels, schematics for future weapons systems, current logistical operations, and petabytes of information needing to be kept private. If the Wiki-leaks or Snowden leaks have exposed anything, it is that the desire to break down the stovepipes between agencies in the intelligence community and the military has increased the vulnerability of secrets.

The U.S. military and intelligence communities are dependent on the efficient exchange and maintenance of data, and as a nation the United States is in desperate need of a decision-making theory able to confront this new digital reality. It is important to consider why traditional models of decision-making are not applicable in the context of the evolution of technology. Before progressing, it is necessary to outline what this book does and does not claim with regard to cyber operations.

All of the information in the preceding paragraphs indicates a growing and inherent value associated with information communications technologies (ICT). The importance of information for every aspect of modern society has grown significantly over the last thirty years. This book does not address the definitional gray area regarding what constitutes cyber war or pretend to assess the full offensive, defensive, or deterrent capabilities associated with actions taken within this domain. While many of the references in subsequent chapters include the topics of conflict and warfare, this book does not explicitly define information operations as acts of war.

This book stands between the linguistic and severity debates and asks how states make rational decisions regarding the conduct of offensive cyber operations, commonly referred to as cyber attacks, within cyberspace. As Jean-Loup Samaan notes, there are those who refer to cyber attacks as the equivalent of nuclear warfare and those that refer to them as annoyances.[32] This book does not take an official position on the range of debates and seeks rather to present unbiased evidence to further progress toward understanding the domain from a nation-state orientation. But before the book focuses specifically on cyber decision-making models, it is important to understand where cyber fits within international relations broadly.

CYBER AND INTERNATIONAL RELATIONS

Johan Eriksson and Giampiero Giacomello considered cyber issues within the broad theoretical framework of international relations and concluded that neorealism provided little help in fully understanding the intricacies of the domain because it fails to understand the interdependent nature of cyberspace.[33] They contend that neoliberalism establishes a more dynamic explanation of the world encompassing both absolute and relative gains.[34] Additionally, they contend constructivism is best applied to the "symbolic, rhetorical, and identity-based aspects of digital-age security," yet that it lacks extensibility to generalize phenomena at the international level, making prediction of state behaviors difficult.[35] To contextualize cyberspace issues related to national security within the broader field of international relations, it is important to recognize that just as each theoretical paradigm offers insights into behaviors among states, the selection of a particular lens through which to interpret the world enhances the rigor of a debate by grounding it in a single heuristic.

The attributes of cyberspace are relevant within the framework of neoliberalism developed by Keohane and Nye in their classic work on international politics, *Power and Interdependence*. Economic and societal interdependencies over the last thirty years have been influenced by technological developments facilitating globalization of economies and information. Increased interdependence has resulted in vulnerabilities and absolute gains. Cyberspace vulnerabilities, as a result of complex interdependence, are a function of an increased reliance on interconnected systems of systems, spanning sovereign spaces, leveraging interoperable information architectures. Cyberspace and its expansion across nations has helped to fuel many of the absolute gains associated with globalization while at the same time providing greater access to information to more people globally than at any other point in history.

When Kenneth N. Waltz wrote *Theory of International Politics*, he wasn't imagining a world where the effective borders of civilian interaction were torn down. In 1979 the Iron Curtain was still firmly in place, and the transmission of information from one nation to another still took time. While ARPANET existed, the World Wide Web did not. Computers were beginning to grow in importance, but their value was still somewhat limited. Interdependence occurred through fairly rigid economic transactions and legal/regulatory frameworks. Even the rise of truly multinational corporations with highly extensively diversified supply chains was still largely in its developmental phase. Power stations and banks were becoming increasingly computerized, but they were largely stand-alone entities. The realist world of non-interdependence predicated on issues isolated to security in the form of relative gains was at its strongest. As connections increased and computerized systems made their way into every-

thing from cars to soft drink machines, the value of those newly networked and digitized tools began to increase the value and interdependence of the international system.

If we philosophically step back, it is possible to claim, as Mearsheimer does, that we are still in a great power politics struggle, yet this struggle is defined by an information environment very different from the one in which neorealism was conceptualized.[36] Security is still preeminent in the eyes of most scholars and still consumes a basic need status, but security is no longer walled off behind borders. Economic systems that support the military capabilities of states no longer have limited contact with their external counterparts. Everything from food security to economic security to nuclear security is now constantly connected to the world around us. These connections are often designed in international forums, such as ICANN, World Wide Web Consortium, the Internet Society, and the International Telecommunications Union, with limited state representation.

Alexander Wendt's argument for constructing international relations, the idea of identity, and norms and ideas developing into societal and international norms is helpful in understanding the normative interactions in a rapidly evolving environment, yet less helpful in managing the complexity.[37] Constructivism offers a nuanced and detailed look at the motivations for how protocols and coding schema evolved to influence the functional interoperable environment of cyberspace. However, constructivism is challenged when attempting to examine the macrolevel interactions of states. The intermediary analysis necessary to aggregate and predict state behaviors limits the usefulness of constructivism for the study of state-level cyberspace decisions.

Realist theories oversimplify the security situation posed by the development of cyberspace, and constructivist theories look too deeply into the inner workings of a system that is so complex that even those who designed it cannot fully comprehend it. Neoliberalism, for the purposes of understanding decisions in international relations relating to cyberspace, is the most applicable theoretical framework.

Neoliberalism allows for a rational decision-making model to develop without getting lost in the milieu of perceptions. The ontological foundations of neoliberalism alter the realist notions on relative gains for security and are of critical importance in explaining an environment encompassing relative and absolute gains. Security issues within an interdependent environment increasing in absolute value with increases in connections cannot and should not be conceptualized within a purely relative gains framework. Because of its dynamic nature, cyberspace, within this work, is examined on the spectrum of theories between constructivist norm development and the realist simplicity in a neoliberal heuristic. The concepts of interdependence and absolute value are of critical

importance particularly when considered in the context of the interconnected nature of modern security, economic, social, and political concerns.

National security depends on cyberspace not only for its C2W capabilities but also for a multitude of systemic interconnections including economic security, environmental security, social and political security, as well as military security. The pervasive nature of the domain makes a direct application of existing rational choice models for conflict imprecise and lacking in explanatory power. Understanding and predicting the behavior of states in relation to offensive cyber operations requires a rational decision model comprised of the component aspects of the decision calculus tailored to the unique domain in which operations occur.

UNDERSTANDING THE DECISIONS OF STATES: THE LOGIC OF RATIONAL CHOICE MODELING

Cyberspace, as the above characteristics indicate, is a domain unlike any of the others. It is a domain that has far-reaching implications across domains and has come to shape the modern world and play a role in the U.S. strategy of "full-spectrum dominance."[38] Because the domain crosses so many layers of national security, and because difficulties regarding accurate attribution within the domain pose so many problems for conventionally oriented security studies theorists, cyberspace challenges traditional decision-making models.[39]

Most security studies works addressing cyberspace fall somewhere between ambivalence and alarmist. Any policy-maker attempting to make a decision regarding the use of offensive cyber weapon systems in a role beyond tools of force communication or multiplication would find that there is a lack of debate on how this new category of weapons can generate political benefits. The cyber domain itself is not easily conceptualized. Whereas a policy-maker can easily understand the implications of launching a missile to hit an intended target, a cyber attack that might achieve the same result is difficult to comprehend. That the same political benefit of a missile attack on a target can be caused by a weaponized thumb drive containing a virus payload sounds more reminiscent of science fiction than science fact. A solid and accurate understanding of how to decide to use a cyber weapon is unavailable to the policy-maker in a clearly formatted and logical structure.

Because the cyber domain is unique from other more conventional domains and is of critical importance to the functioning of the national security of modern states, there is a need for a logical conceptualization of state rational decision processes to influence the policy actions of other states using cyber weapon systems. The power of states in cyberspace and consequences of actions in a networked system of systems environment are not straightforward.

There is a larger degree of consensus on the ability to leverage cyberspace tactics, techniques, and procedures (TTPs) for soft power gain. The U.S. State Department frequently makes reference to cyber and implicitly soft power and has used its influence to provide tools or maintain services for the communication and organization of popular uprisings.[40] Various organizations have identified corresponding online trends associated with large-scale social and political movements that indicate a role for cyberspace in influencing public discourse.[41] Hard power, unlike soft power, necessitates approval by the executive of a state. Whereas applications of soft power are institutionalized and part of an ongoing policy process, decisions to use hard power are not continuous policy processes, but rather moments of extreme contention requiring decision choke points indicating a substantive benefit associated with a specific deliberate action.

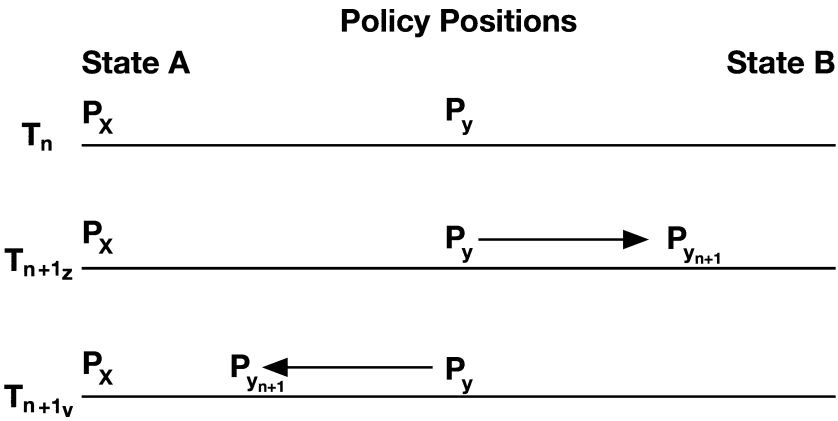
To create a rational decision-making model it is helpful to focus on decisions as points in time rather than an institutionalized decision-making process or a functional system. Because most applications of soft power typically do not require a single decision-maker's approval and because the spectrum of soft power is so vast, ranging from the provision of tools to the creation of targeted media, it is for the purposes of the subsequent arguments largely ignored. This should not be taken to mean that cyber soft power is not of importance, but rather that there are actions within cyberspace that require a unitary decision and clearly constitute an application of hard power.

Hard power and soft power exist on a spectrum. Joseph Nye defines hard power on one end of the spectrum as the ability to command, threaten, or sanction.[42] More simply, he defines the difference between hard and soft power as the difference between "push" and "pull."[43] The decision to use the stick rather than the carrot is typically an executive one requiring a rational decision that weighs the utility of action versus inaction or actions that do not make use of the constitutive aspects of hard power.

The logic associated with the application of power from a state perspective is necessarily situationally and value dependent. As figure 1.1 illustrates, states fall along a spectrum on particular policy positions. State A can have a preference P_x on a particular policy, while state B can have preference P_y. State preferences are not static and can and often do change over time. The process of change can lead states to move either closer or further apart on the spectrum of a particular policy decision. Figure 1.1 is a simplified example of the policy spectrum and shows that often both states in diplomatic relations will mutually influence one another, possibly moving both their positions either closer or further away from one another.

The objectives of hard or soft power are complicated from state A's perspective. State A would like to have state B move closer to its policy position, as this would likely lead to improved relations between the two states. If movement

FIGURE 1.1 Understanding State Policy Positions



State A has a policy position of P_x. State B has a policy position of P_y. In time n+1 state B either moves its policy position further from State A's or closer.

toward state A's policy position is not possible or state B has indicated a desire to move further away from A's policy position, then state A prefers to either slow the movement of state B from its policy decision or maintain the status quo. Either form of power can be used to accommodate this objective.

Is it possible to differentiate between the logic of which type of power to use, and why is it that hard power necessitates a decision-making model with a unitary actor, while soft power does not require such constraints? The distinguishing feature between what necessitates a unitary decision-maker lies in definition of what constitutes hostility. All applications of hard power can reasonably be assumed to constitute hostile acts against another state meant to influence their policy position.

Iran likely thought the maintenance of Twitter networks, at the request of Secretary of State Clinton, during the Green uprisings following the 2009 election of Mahmoud Ahmadinejad constituted a hostile action. Although the act itself was done with little to no aggression and no objective policy goal other than to facilitate an event already in progress, the same could not be said of the moves by the United States to sanction Iranian oil supplies.[44] Sanctioning is a clear political signal designed to force the Iranians to relinquish their nuclear ambitions. The action is hostile and has an expected (desired) outcome, the cessation of Iran's nuclear weapons program.

Building the argument for a decision-making model predicated on the use of hard power has inadvertently created a logical shortcut around an area of major concern for many cyber theorists. Often scholars discussing the use of cyberspace in the context of national security offense and defense get stuck when it

TABLE 1.3 The Cyber Warfare Lexicon

Cyberspace	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Cyberspace Operations	**CO:** All activities conducted in and through cyberspace in support of the military, intelligence, and business operations of the Department.
Cyber Warfare	**CW:** Creation of effects in and through cyberspace in support of a combatant commander's military objectives, to ensure friendly forces freedom of action in cyberspace while denying adversaries these same freedoms. Composed of cyber attack (CA), cyber defense (CD), and cyber exploitation (CE).
Cyber Attack	**CA:** Cyber warfare actions intended to deny or manipulate information and/or infrastructure in cyberspace. Cyber attack is considered a form of fires.
Cyber Defense	**CD:** Cyber warfare actions to protect, monitor, detect, analyze, and respond to any uses of cyberspace that deny friendly combat capability and unauthorized activity within the DOD global information grid (GIG).
Cyber Exploitation	**CE:** Cyber warfare enabling operations and intelligence collection activities to search for, collect data from, identify, and locate targets in cyberspace for threat recognition, targeting, planning, and conduct of future operations.
Cyber Warfare Capability	**CWC:** A capability (e.g., device, computer program, or technique), including any combination of software, firmware, and hardware, designed to create an effect in cyberspace, but that has not been weaponized. Not all cyber capabilities are weapons or potential weapons.
Cyber Weapon System	**CWS:** A combination of one or more weaponized offensive cyber capabilities with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

Source: U.S. Strategic Command, "Cyber Warfare Lexicon."

comes time to define what constitutes an offensive cyber operation. U.S. Cyber Command, a sub-unified command under U.S. Strategic Command, issued a combined lexicon document that facilitates consistent terminology and definitions across the Department of Defense. Although the specific terms are not consistent internationally, it is beneficial to use this combined lexicon as a basis for defining terms in the cyber domain. This document was originally classified, but it has since been released and was publicly posted on the website of the *Washington Post*.[45] Table 1.3 provides a small selection of terms relevant to the current examination of cyberspace in the context of decision-making.

Actions taken in cyberspace to exploit information, digital espionage, constitute cyber exploitation (CE) and do not fulfill the requirement for altering the policy positions of other states. The process of exploiting networks can significantly influence the ability to conduct cyber attack (CA) operations, as is examined in detail in chapter 7, but CE activities do not warrant a decision by a single executive decision-maker. CE operations occur with regularity, and while they are a major vulnerability, they do not constitute an application of hard power. This distinction is made particularly within the field of cyber legal studies.[46]

Patterns emerge when examining political action around the world. States in the international arena engage in various forms of political action to influence other states. This coercive action can take many forms. International relations is replete with studies on sanctioning, threat politics, military actions, and a host of other tangible activities designed to influence the policy structures of opponents.

Scholars, including Geoffrey Blainey and Stephen Van Evera, focus on the causes of war, a prolific area of study within international relations. These and other scholars examine war within the physical/kinetic domain and attempt to define patterns of behavior over a long history of conflicts.[47] Within these patterns they provide explanations, not just of what causes war, but also how to prevent wars. Each scholar identifies common threads identified across the scholarly debate, yet they often diverge when identifying the specific causal variables leading to conflict. Although the security studies field has focused substantial effort on the specific material factors associated with the instigation of conflict such as capabilities, power status of states, borders, and so on, the literature that focuses on the decision processes (both cognitive and rational) that made the calculus of war is far smaller.

Conventional paradigm theorists such as Waltz, Mearshimer, Keohane, Moravcisk, Levy, and others indicate ontological foundations or norm developments as the basis for the conflict trap.[48] States either form institutions to mitigate information asymmetries, engage in conflict due to power struggles, or conform to norms discouraging or encouraging conflict in various situations. But why do states decide to take that first shot in any form of conflict? As the previous section on the connection of cyber to international relations indicates, the answer lies somewhere in the complexity of the power and interdependence argument developed by Keohane and Nye.[49] The paradigm gives a theoretical framework within which to understand the broader issues of cyber in international politics, but to understand the application of force in cyber—why someone was authorized to press the enter key and launch an offensive cyber operation—it is necessary to drill down to the spark or calculus in the mind of the decision-maker.

Carl von Clausewitz is famous for his phrase "War is politics by other means."[50] His famous quote indicates war and conflict are, to a large extent, political acts.

Politics is a zone of bargaining designed to influence others to change their policy positions to fit more closely with one's own policy platforms. The process of politicking can be accomplished in many ways. In any given situation there are tools available to individuals to manipulate conditions to their advantage. International politics is not immune to attempts by states to influence the policy positions of one another to their advantage. Often this occurs in explicit bargaining and diplomacy. States discuss options and attempt to come to a mutually satisfying agreement. There is a range of international institutions facilitating diplomacy. The United Nations, the World Trade Organization, and Mercosor, to name but a few, all play a role in enhancing communication and political interaction between states. Very often these institutions provide the outlet necessary to shift policy decisions among states to an agreeable middle ground. This type of international politics is assumed to be a positive sum game. All parties to a certain degree can walk away from the negotiating table winners.

Security issues often force states into a zero-sum bargaining range. It is in this area that states are apt to resort to hostile tactics. The traditional security studies literature indicates threats and implementation of sanctioning or military action are tools in the toolbox of political leaders to influence the policy positions of other states. As indicated above, these actions largely occur in the physical world and are overt actions. The threat of implementation of covert sanctions is likely to have little or no effect, as the sanctioned party will not know what policy course it needs to take in order to reduce or eliminate sanctions. The same holds largely true with conventional military action. The objective is to provide a visible and tangible coercive strategy designed to alter the policy position of another state.

The use of means other than nonhostile diplomacy to influence the policy decisions of other states requires a decision to be made. This decision is dependent on a multitude of considerations. However, the decision itself is broadly constrained by three generic qualifiers: (1) What is the utility of action? (2) What is the uncertainty that such an action will not work? (3) What risk is associated with this type of action? These constraints weigh heavily on the decision to forgo nonhostile methods of political action in favor of actions likely to be construed as hostile.

It is not complicated to deconstruct the above qualifiers. If a state engages in an action and it is successful, what is the expected gain? Will the target of the action shift its policy adequately in the desired direction? How certain is it that this action will be successful? If a state is highly uncertain its action will result in the desired change, this weighs greatly on the utility of such an action. Lastly, what risks are associated with such an action? Is there a possibility for retaliation? Will this damage the instigator's reputation? Will this impair future attempts with other states? There are numerous subquestions to be asked re-

garding the development of the decision; however, the broad decision matrix is constituted through utility, conditioned by uncertainty, and risk.

There is an understanding that security issues often shift from nonhostile diplomatic negotiating to alternative, more overt coercive forms of political action designed to influence the policy positions of states. But this view of political action as being explicitly overt, as considered by most theorists in security studies, is largely misplaced because for millennia some of the boldest operations and often the ones bearing the best political results are those occurring without the knowledge of the intended target. The conflict over political utility and covert action is examined in exhaustive detail in chapter 3.

The policy process can be broken down into three broad categorizations: (1) nonhostile overt bargaining, (2) hostile overt bargaining, and (3) hostile covert action. Most of the international relations literature focuses on the first two. It is, however, the third type of action, which has gone largely unnoticed in modern theorizing, that has the largest independent political value and is most applicable to the cyber domain.

Sacrifice is required in overt nonhostile bargaining to reach a mutual decision. One or both sides must lose to achieve a political goal in overt hostile bargaining. Yet covert political action offers a third path, one that influences the intended target to achieve a political result, altering policy positions without knowledge and explicit consent. As in chess, it is best to have the opponent think they are making their best move, when in reality they are positioning themselves in checkmate. The broad tenets of the decision to use any of the three types of action are the same. A state engaging in any political action will attempt to define its utility for each type of action, and from there it will chose the best path to take.

Utility is not a complicated concept; rather, it is something human beings do every day without even realizing it. Utility modeling is the mathematical modeling of aspects of a decision. Rational choice utility modeling, largely developed by John Von Neumann and Oskar Morgenstern in 1944, was a means to understand economic decisions.[51] Utility theory essentially states that a rational individual given a series of alternatives will weigh the values of each and create a *complete*, *transitive* preference ordering. This preference ordering makes it possible to quickly and easily discern which alternative an individual will choose.

It is important to note the model works only with individual decisions. This is due to Kenneth Arrow's impossibility theorem, which states that a group of three or more individuals given a set of three or more alternatives cannot rationally order the alternatives.[52] Arrow illustrates that the simple ordering of the alternatives will greatly influence the ultimate decision, thereby negating the relative value of each of the alternatives, and will possibly lead to a suboptimal outcome. Fortunately, for acts of a hostile or covert nature, the ultimate deci-

sion to employ such actions is typically relegated to a single decision maker or head of state.[53]

Autocracies and other forms of nondemocratic societies are most associated with having a unitary decision-maker. One reason states seek regime change within autocracies is to oust the decision-maker and by doing so allow for a new leader who will establish friendlier policies. Yet ironically, on matters of war and peace democracies quite frequently shy away from or minimize their democratic principles. A sign on President Harry Truman's desk read, "The Buck Stops Here!" Crises tend to move democracies away from deliberative democratic debate and toward single decision-maker models. Although the deliberative process has in many instances attempted to constrain the ultimate decision-maker, as seen in the passage of 50 U.S.C. 1541–1548—The War Powers Resolution of 1973—there have been instances where this resolution has been ignored in part or whole.

So why do democracies tend to shy away from their core beliefs during crises? The answer lies in Kenneth Arrow's impossibility theorem, which essentially lays out the breakdown of the decision-making process in groups. What he finds is of critical importance in situations where the utility of the various policy options being vetted can be subsumed in a mathematical maze of sorts, leading to inefficient outcomes. Groups attempting to derive a decision from different options must consider that each member of the group has a unique preference ordering. If all the preference orderings are weighed equally, then the decisions within the group cannot be transitive, or fixed (complete). This leads to a situation in which the utilities of each of the possible options conflict with the utilities of the other options, leading to a circuitous or unsolvable decision process.

Bueno de Mesquita uses the Cuban missile crisis as a hypothetical example of such a decision process.[54] There was a deep division among the administration's leadership over the appropriate response to the placement of nuclear warheads in Cuba. The decision-makers were presented with three primary options: invasion (i), blockade (b), and surgical air strike (s). Bueno de Mesquita asks the reader to assume that an executive committee rather than the president is tasked with determining the best course of action to take. He denotes three groups. Each of the groups has a preference structure: (a) sPiPb, (b) iPbPs, (c) bPsPi. He indicates that the first group prefers the air strike to an invasion or to a blockade, the invasion to the blockade, and on down the line. From this information what is the collective decision of the committee?

The problem in this decision model quickly becomes evident, as the preference orderings provide no clear guidance on what course of action the group supports. Bueno de Mesquita contends that a dominant decision-maker will attempt to impose or bargain his policy position to the top of the list. Using the preferences as defined above limits consideration to only two of the options at a time: for example, strike or invasion. In this instance the decision matrix

indicates that a strike is more prudent. However, if the committee had first attempted to decide between an air strike and a blockade, then the decision matrix would have ended in the invasion being considered. Thus in such a group decision process the order in which the items for consideration are presented greatly influences the eventual outcome, and that outcome is then conversely not dependent on the utility value associated with each option.

The impossibility theorem is a major blow to game theory literature in general and specifically to aggregate decision-making. With multiple options in a group setting, a single rational outcome is unable to be achieved.

Bueno de Mesquita fleshes out this aspect of the argument for a utility model of international conflict in great detail. He highlights that most countries including the United States have provisions that lead to the executive being the final decision-maker in whether to go to war.[55] This is important in the development of a formal rational theory for the employment of a specific type of operation against opponent states, cyber attacks.

When discussing the development of rational decisions by states, theorists are implicitly assuming a single executive. This is not to insinuate that there are not other important actors in the decision-making process. Debates in legislatures, the general public, media, norm entrepreneurs, and other persons of influence all weigh heavily on a decision-making process leading to conflict. However, as Bueno de Mesquita argues, all of these other actors influence the decision process, but the ultimate decision to engage in hostile activities is typically not made by group fiat. If all the actors of a state are warmongers and a single forceful executive finds the calculus of war too costly, it is often he or she alone who can make the decision to avoid war.

This decision is economic in nature and fits accordingly with Von Neumann and Morgenstern's utility models. A parallel economic example is that of an individual deciding between apples and oranges at the local grocery store. The apple and orange industries each attempt to influence the decision of the individual with advertising. Family members might express their preference for one type of fruit or the other. Ultimately the decision between the apple and the orange rests on an expected utility of pleasure or fulfillment derived from purchasing and eating the apple by the individual. This fulfillment is relative to the cost associated with each of the types of fruit. The consumer, as a rational actor, might have a strong preference for apples and only switch to oranges when the relative cost of apples exceeds the expected value of that apple relative to the cost of an orange.

The above example is simple, yet it is meant to illustrate that the decision process in many situations, though not all, boils down to an individual decision-maker. Further examples of an executive having the final say in the instigation of hostilities can easily be found within modern history. In 2011, President

Barack Obama unilaterally without the consent of Congress instigated hostilities against Libya. During World War II, elections were suspended, providing Winston Churchill with a well-defined executive power over the duration of the war. In dictatorships the relationship between the rational instigation of hostilities and the single decision-maker is less confusing. Democracies typically shift away from consensus or majoritarian decision-making during hostilities.

A valid question is why does this really matter in the context of the three options listed above with regard to the broad classifications of international interaction being either bargaining, hostile overt action, or hostile covert action. If we are trying to understand the decision-making process of any of these aspects, we have to understand the relation between how we decide to use them and the utility that can be derived from such an application.

Decision-makers are in essence weighing the options of these three broad paths to influence the political environment. The ability to decide which path to take is based on a fully rational understanding of the value of each of the paths. Each of these options contains risk and uncertainty over whether it will achieve the desired change and create the political utility desired. It is by deconstructing this complex nested decision process that states are able to understand whether it is better to maintain normal international relations through diplomatic action or engage in alternative means to shift the policy preferences of others. The emphasis in the following chapters is on the two paths diverging from the diplomatic. These two paths are closely intertwined and often overlap either intentionally or accidentally. Specifically, decision-makers are presented with a new set of tools, which can influence the decision to use one or both of these paths. These tools fall within the new and man-made cyber domain but have very real and tangible aspects felt in the physical world.

If we know a unitary decision-maker bases decisions on a utility calculus, and that this calculus is utility maximizing within rational choice, what necessitates a new study on decision-making within the cyber domain? Bueno de Mesquita isolated the patterns of how leaders decide if an overt war is rational or not, but his model is largely predicated on qualities not pertinent or applicable to cyber. His utility function is constructed on the overt nature of the international community with regard to declarations of war, peace, and understanding the interactions among states. His study reduces the error of predicting when a state will initiate a conflict and whether that state will win. His model is more successful than many of its pure power score counterparts and provides a logical chain of thought. This logical chain of thought is still applicable in the realm of conventional military action. Yet, this is only one part of the story of international politics.

Scholars have developed theories of diplomacy and of conventional conflict initiation, but those are not the only ways to influence the policy positions of

states. They have not been the only ways to influence the policy positions of states dating back many millennia. As such, the picture they provide us is woefully inadequate. Scholarship currently stands like a deer caught in the headlights of major conflict and overt diplomacy, ignoring those hostilities that go unacknowledged yet create a large amount of political utility.

This book particularly contends with the utility of one type of covert action—cyber attacks (CAs) in the form of offensive cyber operations (OCOs). Beyond merely the consideration of the covert versus overt nature of options available to states, the cyber domain offers up a unique set of challenges to Bueno de Mesquita's model for the development of utility in a decision-making process. Conventional domain conflicts are currently analyzed using Bueno de Mesquita's rubric by using Composite Index of National Capability (CINC) scores affected by monotonic declines in power over distance. His rationale for this measure is logical and well reasoned from a traditional conflict decision-making perspective. A state that is better endowed with resources than its potential adversary has a higher probability of being successful in a conflict. The farther a state attempts to extend its power and resource capabilities out from its center of gravity, the more its relative power begins to decline.[56]

For the cyber domain it is inappropriate to use CINC scores or monotonic declines in power over distance. In addition to these two inappropriate attributes, cyber adds complexity of anonymity and attribution. These additional characteristics necessarily qualify CA as a covert act to be examined in more detail in chapters 3 and 6. Why are CINC scores an inappropriate measure of cyber capabilities? Their inappropriateness is not hard to discern. CINC scores were first developed by David Singer in 1963 and have been used since as a measure of national power in the Correlates of War (COW) project.[57] When they were first developed and for first half of their history, the cyber domain was of little concern. More importantly, for the types of conflict examined within COW they are applicable. As states become increasingly interdependent and their national securities are evermore tied to cyberspace, the power relationship within the conventional domains has become increasingly limited in its explanatory power for this new form of conflict.

CINC scores incorporate measures of total population, urban population, iron and steel, primary energy, military expenditure, and military personnel. Each of these is an important consideration in conventional warfare and particularly in the decision to engage in hostilities. Cyberspace, however, is logical, physical, and social, meaning that total population, or urban populations, or any of the other constitutive parts of CINC scores do not adequately measure power in this domain. Cyber power, which is examined in chapter 4, is constructed by analyzing offensive and defensive technological strengths and weaknesses as well as dependencies leading to vulnerabilities. The power of these strengths

and weaknesses does not monotonically decline over distance, as operations within cyberspace are almost instantaneous,[58] and there is little to no necessity in moving cyber units around the world for the majority of operations. An operator can sit at CENTCOM (U.S. Central Command) and fly a drone over Afghanistan thousands of miles away with no loss of effectiveness or lethality.[59]

Beyond the inappropriateness of conventional measures of power is the way risk is formulated. Because the probability of success in conventional hostilities is relatively straightforward in pure military capability terms, it was adequate to use pure national military capability measures. But cyber, as with many other forms of covert action, has added attributes influencing the probability of success for any type of attack. For simplification purposes this book combines the anonymity-attribution problem. In reality it should be parsed out based on intelligence, as is illustrated in chapter 7. A conventional domain attack is relatively unavoidable even if it is known beforehand. Iran cannot easily move its enriched uranium production facilities even if it knows Israel is about to attack. It can harden its facilities and attempt to weather an attack, but it cannot nullify an attack. With cyber attacks, if a specific type of attack and where it is coming from are known, the defender can minimize or nullify its effect.

A server or computer with information on it and connected to the Internet is much like a ship in the ocean. The ship is fine so long as it knows the weather conditions in advance. The captain can steer the ship to safer waters or, in the event of a hurricane, can dry-dock or harbor the ship. The same is essentially true of a country under imminent threat of a cyber attack from a known source. A network administrator can thwart an attacker in a number of ways if the identity of the attacker and the timing of the attack are known. In a worst-case scenario the administrator can effectively dry-dock the network by removing external connections or temporarily shutting down systems. There was even a bill proposed in the United States Congress promoting the idea of an "Internet kill switch."[60] Because cyberspace is characteristically different from conventional forms of hostilities, a decision-making model needed to assess the utility of an attack employing cyber tools, known in military vernacular as cyber weapon systems, as uniquely different from conventional military weapon systems. The development of utility in a cyber decision-making model necessitates modified variable attributes and probability development. This modification in the development of probabilities greatly influences the subsequent development of political utility within Bueno de Mesquita's original theory.

Lastly, Bueno de Mesquita's model is largely based on state alliances. However, because cyber action occurs covertly at least in the initial stages, the consideration of alliances, while important, becomes mathematically irrelevant as the utilities for the actors are created independently. This book therefore modifies the underlying probability functions associated with the utility theory devel-

oped by Bueno de Mesquita. It remains firmly within his bilateral modeling of international conflict and finds that cyber attacks by states are most commonly covert actions using cyber weapon systems to engage in offensive cyber operations and to achieve limited positive utility.

HOW THIS BOOK IS ORGANIZED

This book builds and tests an argument on the ability of states to make rational decisions regarding actions to use cyberspace to achieve political utility. Beginning in chapter 2 the focus becomes the importance and attributes of the cyber domain. Chapter 3 examines the motivation for and utility derived from cyber attacks. Chapters 4 through 6 focus on the attributes of the probability of achieving political utility when engaging in offensive cyber operations. Each of these chapters takes one part of the calculus and examines it in detail. Chapter 4 defines cyber power and vulnerabilities. Chapter 5 examines the concepts of attribution and anonymity and proposes methods for accounting for anonymity and attribution issues when engaging in OCOs. Chapter 6 examines the relationship between conventional conflict and cyber conflict and attempts to isolate similarities and differences, at the same time highlighting areas where they are mutually supportive. Chapter 7 acknowledges the open source nature of this book by providing a logical framework for the inclusion of intelligence analysis to aid in developing this model to its fullest. Chapter 8 formally introduces the modified Bueno de Mesquita model by putting together the pieces of the probability components developed in previous chapters and testing them. Chapter 9 challenges the fundamental argument of the book by presenting alternatives using prospect theory and construal level theory. Chapter 10 examines the current status of cyber decision-making in the United States and examines how jurisdictional and legal authorities hamper both the rational model and cognitive models and explains the importance of a formal decision-making model in providing policy-makers and scholars alike a foundation upon which to build further study.

CHAPTER 2

The Key Concepts of Cyber

THERE IS A GROWING societal and military reliance on all things cyber. Yet this reliance is often difficult to see. It invades our lives slowly until we forget when we first came to depend on mobile phones, or we can't remember the last time we couldn't look up the answer to something on Google or another search engine. Whereas the previous chapter began by highlighting the evolution of a new domain of operation by comparing it to land, sea, air, and space, this chapter takes the next step and focuses on the first part of chapter 1 by answering two questions:

1. Why is cyber important to national security?
2. Why is the cyber domain inherently asymmetric?

These two questions build upon one another. The first question is answered by identifying the four pillars of national security: political and social, economic, military, and environmental. Combined, these pillars have been heavily influenced by information communications technologies and the proliferation of computing devices. Yet influence alone is not enough; instead, these devices, connections, and the work processes they have created have generated far-reaching national security implications. The implications are now embedded in pillars and have constructed overarching network architectures that blur the traditional conceptualizations of military versus civilian targets. What is intrinsically fascinating about changes that the cyber domain has brought and continues to bring to bear on national security is that we have largely created systemic dependencies for ourselves, because the cyber domain, unlike its counterparts, is man-made. Our man-made domain continues to evolve as we as humans continue to connect, to develop, and to improve each part of the network of networks. In many ways this process of connections and developments in code and hardware are not business-like structures but rather are more analogous to organic evolution.

The second question on the asymmetric nature of cyber is only unique to cyber in the relative power potential for asymmetric interactions that can be highly pronounced within the cyber domain. Asymmetric conflict is relevant to all domains of conflict; however, asymmetry has specific qualities in the cyber domain. Although some of the characteristics of asymmetry in cyber are reminiscent of other domains, most of the attributes are unique due a decentralized

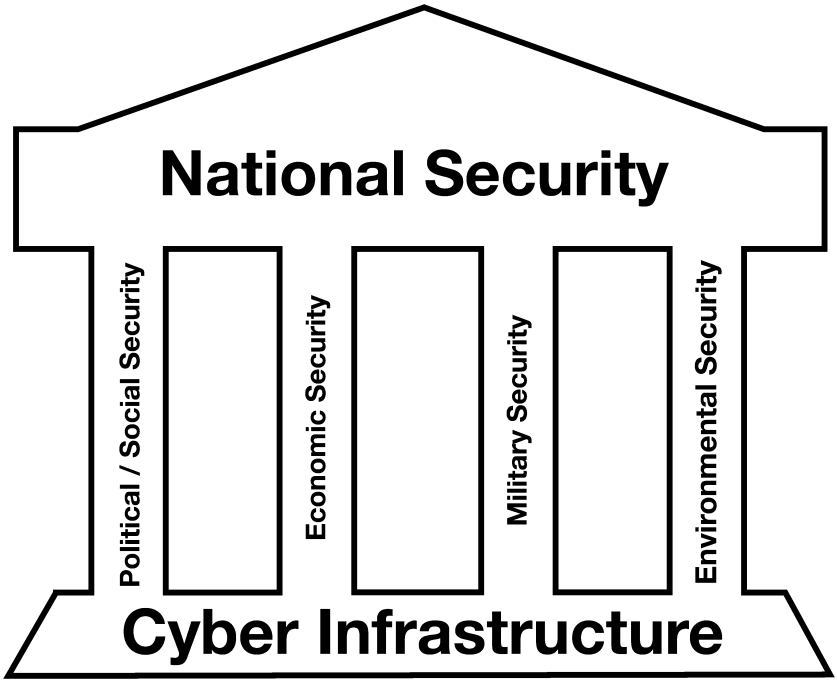
man-made environment. Asymmetry in any domain affects the decision-making process of leaders and conditions how they respond to events that arise. However, the complexity of asymmetry and the David versus Goliath problems potentially present in the cyber domain portend far-reaching ramifications. The focus here is on the dependency of the state on cyber, the interaction of cyber with a broad spectrum of modern military and intelligence affairs, and the inherent asymmetry present across nations and other actors within cyberspace.

WHY IS CYBER IMPORTANT TO NATIONAL SECURITY?

National security is the maintenance of the survival of the state. Cyber is important because it forms a modern infrastructure beneath the pillars supporting national security. Cyber infrastructure facilitates the connections of individuals, computers, systems, and, at the most basic level, ideas to one another. As a child grows from an infant to a toddler and then into a young person, his or her cerebral development facilitates the creation of new neural pathways. This progress is amazing to watch, as any parent can tell you. An infant has jerky motor movements and is controlled by basic needs, a toddler begins putting together smoother movements, a child can put those movements into actions like kicking a ball or running, and an adult does not even notice the process. The cyber domain is a connected domain. With each new connection the development of the network increases in value, and our relationship to the connections becomes second nature. Similarly, these neural pathways allow us to control the environment around us. Not only do our connections facilitate our individual actions, but they become the framework for controlling production and economic processes. The connections and the control that follows become enablers. We become dependent upon these connections without even realizing our dependence.

Control goes beyond connection and facilitates action beyond the network itself. Networked controls allow robotics to construct products in factories, manage train and traffic systems, prevent airplanes from crashing into one another, and much more. While control is built on connections, the controlling components of the cyber domain, computers, can take the connections and apply them. Whereas connections primarily facilitate information transmission, computing devices take the information and become managerial or productive. The most commonly referenced control mechanisms within cyber are supervisory control and data acquisition (SCADA) systems or programmable logic controllers (PLCs). These two devices take in information through connections and turn that information into processes. The increases in connections also increase our dependency upon those connections. The more our dependency increases, the more vulnerable we become.

FIGURE 2.1 The Modern Structure of National Security



The cyber domain has embedded itself as a foundation into the national security of states. Broadly, this creates four pillars of dependence. These pillars form a structure of dependence supporting national security. Figure 2.1 illustrates the structural dependence generated through the development of cyber. The connectivity and control of the cyber domain has influenced political and societal, economic, military, and environmental security. The relationship of information communications technologies within each of these categories to national security is complex, yet it can be illustrated through a diverse set of examples.

POLITICAL AND SOCIAL PILLAR

> The realpolitik of the new era is cyberpolitik, in which the actors are no longer just states, and raw power can be countered or fortified by information power.
>
> David Rothkopf, "Cyberpolitik"

Ideas are the lifeblood of politics and society. The control of ideas has for millennia been a strategic objective of rulers and later governments alike. The speed

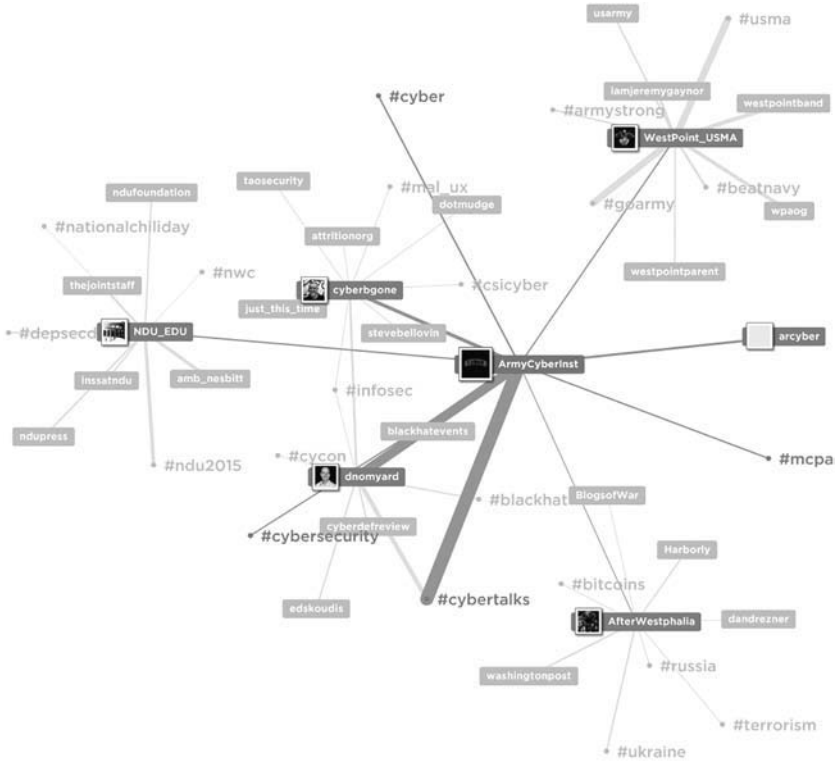
and quantity of ideas has significantly increased in the last thirty years. Information communications technologies have facilitated an information revolution that far exceeds the previous information revolutions of the written word, the printing press, the telegraph, the wireless, and television. While the inventions of ARPANET and later TCP/IP protocols were not necessarily intended to facilitate the transference of ideas, the connecting of computers has had enormous repercussions.

International Relations literature provides a basis for understanding the concept of information transference largely through neoliberal institutionalism. Keohane and Nye in their seminal critique of realism identify complex interdependence as the driving force in international politics.[1] This interdependence is driven by an increase in the number of channels of communication between nations and within nations and the flattening of the hierarchy of political issues of importance. They indicate that the interconnections and the flattening of the hierarchy of issues reduce the need for the applicability of military force. Complex interdependence has been put on steroids in the cyber world with the near-exponential increases in connections across societies. This complex interdependence has had a profound effect on more than just the transference of ideas; it has reshaped the forum in which those ideas are exchanged.

Yochai Benkler writes of a fundamental change in the public square.[2] The conventional architecture of the public square was hub-and-spoke; this has since evolved into a modern architecture of multidirectional connections. This, he says, combined with elimination of communications costs as a barrier for discourse, dramatically widens the political environment. Daniel Drezner and Henry Farrell reiterate this sentiment when they write of the evolution of a "web of influence" particularly in news and information published within the blogosphere.[3] Figure 2.2 is a graphical representation of the diffusion of information from the Army Cyber Institute's Twitter account on 8 April 2015 following the release of new articles on their blog, the *Cyber Defense Review*. The figure only represents one level out of diffusion. Any of the nodes could in theory contain multiple other topical connections to other nodes. However, it illustrates how quickly information from a nonconventional source can spread, forming an ever-growing web of connections on topics ranging from cybers to human rights and beyond.

Fabien Miard brings the importance of information communications technologies (ICTs) for civil development more clearly to the forefront.[4] He finds that mobile phones act as facilitators of mobilization and collective action for political purposes.[5] The facilitation of civil society strengthens national security, a theme reiterated by A. Lawrence Chickering.[6] The diffusion of information is simultaneously a strength and a weakness for the national security of some regime types, as evidenced by recent revolutions across the Middle East and North Africa, Ukraine, and Hong Kong.

FIGURE 2.2 Graphical Representation of Information Diffusion in the New Public Square



Deborah L. Wheeler indicates the evolution of the public forum and its subsequent impact on national security, while not directly caused by the creation of ICTs, can, given the right spark, facilitate revolutions.[7] This facilitation of political and societal revolutions by information technologies has increasingly become a tool of state power. This state power can be wielded by opposing states as a tool of soft power. In 2009, Iranian activists organized and coordinated massive demonstrations across Tehran using the popular microblogging network Twitter. When Twitter planned to take its service off-line temporarily for a service update, the U.S. secretary of state stepped in and asked them to delay the update until further notice.[8] Although the revolution did not succeed, the episode illustrates the hope presented by these technologies to policy-makers in the United States as tools for social and political change.

There are an increasing number of tools that allow citizens in oppressive regimes to avoid surveillance laws and practices and engage in citizen mobilization. Tools such as Tor and Tails route Internet traffic through the Tor net-

work to obscure a user's web traffic.[9] Tools from the Guardian Project allow encrypted phone conversations, secure chat and text messaging, the elimination of metadata on photos, and much more.[10] Many of these tools are just the beginning and are vital to the sustainment of democracy movements in many countries. Yet, at the same time, these tools subvert the established authority of many states.

Information communications technology has affected political and social movements through its communicative ability to expand the public forum. As the examples above indicate, this can be a stabilizing and destabilizing factor. The communicative capacity of states themselves is also dramatically affected by the rise of ICT. Kristen Lord highlights the problems embedded in the increasing facilitation of transparency by ICT. She contends that despite almost universal claims that transparency in government is a good thing, decentralizing control over information and empowering individuals and organizations, transparency can significantly hinder domestic and international political actions.[11]

Of particular concern to Lord is the role transparency plays in diplomacy.[12] Transparency in diplomacy can have a constraining effect on governments, particularly democratic governments. Although constraints in many instances are of great value and can prevent leaders from making poor decisions not in the interest of the domestic public, often this transparency limits the ability of governments to build mutual trust. ICT has forced governments to become their own public affairs firms in a vain attempt to control their desired message. Often this message is subsumed in the mix of information, much of which may be inaccurate or biased. Examples such as the diplomatic cable leaks by Bradley (now Chelsea) Manning to WikiLeaks also indicate that sensitive communications between governmental departments might not stay secret and can affect a state's relationship with its peers.

ICT can in many instances enhance national security through increased democratic evolvement, monitoring of leaders, and development of complex interdependencies; at the same time, it poses many threats. The connections made within cyberspace are an evolving field of study in domestic politics and societal interaction. The ultimate outcome is still uncertain. What is certain is that the communicative capabilities developed in the last thirty years are affecting this pillar of national security. Because the cyber connection associated with the social and political pillar of national security is not entirely systemically necessary for the operation of social discourse and the dispersion of ideas, it poses a lower level of threat to national security than the other pillars of dependence. However, as cyber becomes more and more ingrained in the development of social and political issues, it will become increasingly important for national security.

ECONOMIC PILLAR

> The healthy functioning of cyberspace is essential to our economy and our national security.
>
> George W. Bush in *The National Strategy to Secure Cyberspace*

Cyber has come to undergird modern economics. Modern global economics, according to Thomas Friedman, has been flattened by cyber.[13] This flattening makes it possible for multinational corporations to expand their supply chains with electronic data interchanges (EDIs) around the world, traversing physical borders using the relatively borderless expanse of cyberspace.[14] Multinational corporations are not the only beneficiaries of this digital revolution; small businesses and individuals are now able to connect and gain access to information and products from around the world.[15] More than facilitating the process of globalization, the information communication technologies of cyber have become the backbone of everything from currency markets and stock exchanges to production lines. It is now possible to order stock on the NASDAQ from Beijing with the click of a mouse.[16] Not only does this expand the possibility for global investment, but it also diversifies and spreads out the risk of investments. The functioning of modern finance and economics is wholly dependent on ICT. This dependence has had far-reaching effects on both the management and the stability of economies. ICT dependence has created increasingly complex transnational interdependencies.

The direct control over financial systems and markets combined with the rise in information technology has also affected regulatory and fiscal controls once previously the purview of national governments. Central banks are no longer fully able to control domestic markets. Part of this is clearly due to globalization, but globalization is largely due to information communications technology. The adage that if one economy catches a cold the world economy gets sick follows directly from the interconnection of global markets within a connected information environment.[17] No longer are markets isolated from one another; they directly impact one another. The disruption of supply chains by natural disasters can cause ripple effects through entire industries.

While the risk on investments is diversified, the risk associated with the systems that facilitate those investments has grown. Bank accounts and transactions are digital data points stored in databases. John McCarthy and his colleagues assert global finance and economics are based on the trust of domestic and international stakeholders.[18] This trust is predicated on the security of the information contained within the economic systems and financial networks. If this information were to be violated, modified, or destroyed, the consequences would be significant and could lead to significant drops in market capitaliza-

tion or revenues, as was demonstrated in the Target Corporation data breach of 2013.

Criminal cyber exploits are not new. The scale and cascading corporate and societal ramifications of these attacks are growing in leaps in bounds. The first-order effects on a company victimized by a serious cyber exploit can be run in the billions of dollars due to post hoc security efforts, emergency marketing, legal and regulatory costs, and stock devaluation.

In 2013 Target Corporation lost information on up to 70 million customers.[19] The data breach resulted in the resignation of Target's CIO and CEO, more than ninety lawsuits, more than $61 million over a several month period in response efforts, and a 46 percent drop in holiday sales from the previous period.[20] The fallout also resulted in a 13.5 percent (approximately $5 billion) drop in market capitalization over the subsequent three-month period.[21]

The second-order effects of the Target incident also run into the hundreds of millions of dollars. The Consumer Bankers Association and the Credit Union National Association estimate the cost of replacing the 70 million credit cards as upward of $200 million.[22] These estimates fail to account for the revenues lost from transactions delayed by customers unable to purchase goods and services with compromised cards.

Financial transactions ranging from retail to market exchanges depend on trust, so the inability of a corporation to safeguard that trust has enormous ramifications. Cyber attacks are no longer just the concern of governments, and individual companies big and small must consider how to safeguard their networks and the assets within those networks.

With the connection of stores to global supply chains comes the added risk associated with vulnerabilities at any given store affecting the corporate infrastructure. The Target cyber incident is a case study in how something as mundane as HVAC access to the network inadvertently compromised the point of sale systems across the corporation. The incident and its breadth should serve as a wake-up call for corporate actors to begin examining corporate policies, cyber security strategies, and governmental lobbying efforts.

In 2013 the White House released Executive Order 13636 to incentivize owners and operators of critical infrastructure to develop more robust cyber security. Yet this executive order relates directly to critical infrastructure and does not directly address corporate America. Corporations could take this executive order as a model for lobbying Congress and the executive branch for policies that can substantively enhance cyber security across noncritical corporate actors. Incentives such as liability and legal benefits, streamlining of security regulations, subsidies, and tax incentives would forward corporate efforts in the long run and develop a market-based approach toward mitigating risks where costs are presently deemed too high.

Corporations can presently participate in Department of Homeland Security information-sharing activities within the constraints of ensuring security for proprietary corporate assets and strategies, consumer privacy, and corporate integrity. Although it might be beneficial in the short run to avoid reporting a potential vulnerability or breach, the cascading effects across corporations and financial entities can make a problem in one company directly relevant to other corporations.

Although the Internet of Things and global supply chains facilitate efficient inventory management and financial record keeping, it is important for corporations to develop systems with built-in software and hardware segregation points able to slow or mitigate the spread of attacks against global corporate cyber infrastructures. All corporations currently exist in a high-threat cyber environment. Although the severity of threat can vary at the margins, it is important to recognize that the policies developed at the corporate level for cyber security must be constantly analyzed and assessed with each new cyber incident both internally and externally. Policy development needs to occur both at the corporate and national levels. Policy development at the corporate level should be specific to the individual needs of each corporation within its risk matrix. National policy development should also be of priority for all corporate actors, as national policy development can foster systemic improvements in cyber security.

Furthermore, because many of the corporate secrets of businesses are digitally stored or transit cyberspace in e-mails, they are increasingly susceptible to digital espionage. National Security Agency (NSA) insider Jack Brenner states bluntly that the U.S. economic, financial, and business infrastructure is one of the primary targets of economic espionage, further increasing the risk associated with the move to cyber.[23]

The vulnerabilities posed by the move of economic systems into the digital realm places the trust of domestic and international stakeholders at risk. This risk is justified on the basis of increase in economic efficiency and productivity. However, as indicated in chapter 1, if the electric grid goes down, all normal economic transactions halt. This is not a figment of the imagination. America's largest retailer, Walmart, uses an inventory management system that tracks the sale of every single item on its shelves, and when a store sells out of an item it automatically orders more.[24] If these supply chain mechanisms fail, the inventory of major corporations could run dry.

The ties of the economy to cyberspace enable high degrees of efficiency so long as the systems function properly. If the systems fail or are hacked, or if data are manipulated or stolen, the economic repercussions can dramatically affect stability and cause markets to crash and CEOs and employees of companies to lose their jobs. A modern market crash caused by a cyber attack would achieve

the equivalent of a weapon of mass destruction, without destroying any physical property. Such an attack could cripple industrialized countries reliant on ICT and paralyze their societies.

The modern economy is also increasingly digitized through E-commerce. The Census Bureau, which tracks sales, indicates that in 2012 E-commerce made up almost a whopping 51.9 percent of all manufacturing shipments, accounting for approximately $3.0 trillion.[25]

The advance of ICTs into economics has profoundly affected the national security of states. It has brought states closer together and confirmed the complex interdependencies proposed by Keohane and Nye. Yet at the same time this interdependence relies on a man-made system vulnerable to exploitation in more ways than ever before. Advances in interdependence are not always symmetrical across nations, as is examined later. Not all countries are as tied into cyberspace. Often countries that are lower on the aggregate developmental scales of the World Bank and other monitoring organizations lack the physical infrastructure and capital investment that make cyberspace of such importance. Those countries that are heavily reliant on cyberspace have an incentive to discourage any significant disruptions in the existing system. Although there is a high degree of asymmetry in cyberspace in terms of usage between developed and developing nations, as the percentage of global population online increases, the relative asymmetries will decline. The economics pillar of national security rests on the assumption of stability. Any source of instability generates uncertainty, and the digitization of economics contains many potential vulnerabilities.

MILITARY PILLAR

Military security refers to the defense of the state against potential adversaries. Douglas Dearth writes, "advanced militaries rely more than ever in modern times upon the civil national, and increasingly international transnational infrastructures."[26] This reliance on infrastructures of both a civilian and military nature create well-known vulnerabilities for the military security pillar. The increased communication and efficiency of the battlefield designed to reduce or eliminate what Clausewitz called the "fog of war"[27] and ever more networked military planning, logistics, human resources, acquisition, and command and control uses of ICTs and their related technologies have fed into a cycle of perpetual vulnerability development that the U.S. government has only recently started to address through the creation of U.S. Cyber Command and the various branch commands associated with cyber.

As discussed in chapter 1, the increasing reliance of modern militaries on information communications technologies has created the modern principle of

command and control warfare (C2W). C2W is largely traced back to the first Gulf War, which is often referred to as the first information war.[28] C2W is an important concept of war and has affected the way in which wars are conducted. Yet, at a more fundamental level, the evolution of military security has made it increasingly reliant on cyber infrastructure for every aspect of its operation. This trend is mirrored by the civilian world. The Defense Department's Joint Vision 2020 outlines the movement toward a digitized military.[29] The vision of a digitized battlefield is one that comprises dominant maneuver, precision engagement, focused logistics, and full-dimensional protection.[30]

C2W is increasingly facilitated by the digitization of intelligence processes including the creation of Intelink,[31] Intellipedia, and other intelligence dissemination tools providing real-time battlespace knowledge. Nick Cullather, citing intelligence community agencies, indicates that the future vision is to provide pilots in the air and soldiers on the ground with integrated combat information.[32] The military-industrial complex has latched on to the idea of connectedness and has begun working in earnest on projects attempting to further enhance the progression toward C2W across all operational domains.

The connectedness of modern militaries has been cited as a revolution in military affairs.[33] Beneath this connectedness is the networked infrastructure itself. Military and civilian systems alike rely heavily on electricity. The modern electric grid, according to a 2011 MIT study, is best thought of as a system of systems increasingly vulnerable to attack.[34] The electric grid also powers sewage and water treatment facilities, supports hospitals, and provides electricity to air traffic controllers and many more aspects of critical infrastructure. More importantly, each of the devices listed in the previous sentence is attached to SCADA systems and PLCs to manage their efficiency and to prevent accidents. Although many of these systems have redundancies, they are of critical importance to the military and civilian communities, and disruptions in these systems can significantly degrade or even possibly damage national security.

Beyond military reliance on services such as electricity, the military relies on cyber to conduct virtually all aspects of modern combat. As former deputy secretary of defense William Lynn wrote in *Foreign Affairs*, "Information Technology enables almost everything the military does: logistical support and global command and control of forces, real-time provision of intelligence, and remote operations."[35] The need for maintaining the critical infrastructures upon which military and civilian infrastructures depend is such a problem that the DoD established a new sub-unified command, United States Cyber Command (USCYBERCOM), to manage the defense of networks. One of many aspects that General Keith Alexander cites as a reason for establishing this new command is the protection of the defense industrial base and the safeguarding of the technological tools that provide for national security.[36]

Penetrations of DoD networks potentially compromise operational readiness of the military by introducing risks and threats to critical mission assets such as logistics, planning, C2W, and integrated communications. Incidents such as Titan Rain, an attack that focused on the Defense Information Systems Agency, the Redstone Arsenal, the Army Space and Strategic Defense Command, and several computer systems critical to military logistics, have the potential to severely degrade the effectiveness of military security.[37] Military security has largely become a coordinated effort between foreign and domestic actors all providing for the physical defense of states. Information communications technologies, industrial control systems (ICS) along the gambit of technologies that are leveraged by the military, can enhance conduct of war, yet they offer many challenges to planners. The national security implications of the digitized military and the need for robust defenses both in the conventional domains and the cyber domain make the military pillar of vital importance to national security.

ENVIRONMENTAL SECURITY

The final pillar supporting national security in the evolving digitized world is environmental security. Although it might seem difficult to conceptualize the environmental pillar's relationship to the cyber domain and national security, the connection is clear. The cyber domain does not control the weather, but weather can affect the cyber domain, and networked technologies are the vanguard of information on potential environmental issues from hurricanes to earthquakes. Moreover, networked technologies control many of the systems that manage chemicals, nuclear fission processes, locks, and dams, and catastrophic damage would result should their systems falter. Beyond the control of the systems that monitor wastewater, nuclear power plants, and the navigation of oil tankers, cyber is also immensely dependent on environmental security in the form of fossil fuels, renewable energy, and more, creating a symbiotic relationship. Because cyber is a man-made domain, it is heavily reliant on electricity for its connections and control mechanisms. Solar storms, large weather events, and natural disasters can all impact the flow of electricity and by extension can dramatically impact the cyber domain. Environmental security is of critical importance not only to maintain cyber infrastructure but also to prevent man-made disasters from occurring.

Each of the pillars props up national security and supports the survival of the state. The dependence on the cyber domain embedded within each of these pillars has largely become second nature. Just as the development of neural pathways occurs as a child ages, national security has developed networked connections that make it function. Damage, degradation, or disruption of any of these pathways also damages the national security of a state.

WHY IS CYBER AN INHERENTLY ASYMMETRIC DOMAIN?

The cyber domain impacts national security and helps form an infrastructure supporting it. Particularly pronounced within the cyber domain is the concept of asymmetric threats. Throughout history there have been few conflicts fought between two sides, man for man and weapon for weapon on opposing lines. War is typically asymmetric. The severity of asymmetry can be small or can be extremely pronounced, as in the U.S. War on Terror. Traditional literature on war contends that conventional conflicts examine asymmetry as a straightforward mathematical function. The belligerent with the better military capabilities has a higher probability of victory. Disadvantaged combatants are taught to exploit the weaknesses of their opponents on the field of battle, to move faster, to blend into local populations, and to strike key choke points. Conventional asymmetry is dealt with through advances in technology, strategies, and tactics. The asymmetries of strategies, tactics, and technology gave the Roman legions an advantage for hundreds of years. The Mongols were advantaged by their agile horsemanship and archery skills. The armies of Napoleon had superior organization and unit cohesion. The British developed the square. Good strategies, tactics, and technologies are tools of advantage. But within cyber the tool is both a strategic asset and a vulnerability. To understand cyber's contextual importance within national security, it is vital to parse its complex relationship with the advantages and vulnerabilities. This section focuses on why cyber is an inherently asymmetric domain of operation and how these asymmetries are unique.

Asymmetry in cyberspace has risen to the level of national policy and was included in the Department of Homeland Security's 2009 *National Infrastructure Protection Plan*. The *International CIIP Handbook* cites the U.S. fear of being caught off guard by asymmetric threats.[38] Network defenders often find themselves at the mercy of asymmetric attacks instigated by an individual or a small group leveraging decentralized capabilities. A system or network maintained to 100 percent perfection only requires one previously unknown vulnerability called a zero-day exploit to fall victim to a potential attack. Asymmetry in financial terms can be the millions of dollars spent maintaining a network and patching known vulnerabilities versus the lone bad actor who has identified a zero-day exploit in his garage. Yet asymmetry in cyberspace is not just associated with bad actors; it can also be a self-imposed vulnerability. It is therefore necessary to clearly define what asymmetry is and then to hone the relevance of the concept for use within the cyber domain.

Steven Metz and Douglas V. Johnson III define asymmetry as follows:

> In the realm of military affairs and national security, asymmetry is acting, organizing, and thinking differently than opponents in order to maximize one's own advantages,

> exploit an opponent's weaknesses, attain the initiative, or gain a greater freedom of action. It can be political-strategic, military-strategic, operations, or a combination of these. It can entail different methods, technologies, values, organizations, time perspectives, or some combination of these. It can be short-term or long term. It can be deliberate or by default. It can be discrete or pursued in conjunction with symmetric approaches. It can have both psychological and physical dimensions.[39]

This definition is broad yet encompasses a wide range of concepts. Metz and Douglas and later Nir Kshetri go on to discuss positive and negative types of asymmetry. Positive asymmetries are strategic/tactical advantages one country has over another. Negative asymmetries are advantages that a country's opponent has over it. Because asymmetry is such a frequently used word it is helpful to pare down the scope of its meaning in the context of cyber. Positive asymmetry in cyber refers to cyber technologies that provide an advantage over potential opponents; more specifically, such asymmetry refers to the potential vulnerabilities present with an opponent's systems. The manipulation of zero-day vulnerabilities found within the PLCs that controlled the Iranian uranium enrichment centrifuges would be consistent with an asymmetric exploit.[40] Instead of the centrifuges being hit with a bomb, they were hit with code at a weak point. Negative asymmetry constitutes a weakness in systems that an opponent is likely to target. The Titan Rain exploitation of confidential information on U.S. defense networks would be consistent with this type of vulnerability.[41] At its most basic, a positive asymmetry is an offensive advantage, whereas a negative asymmetry is a defensive advantage.

A November 2010 Chatham House report summarized best the problem of asymmetry in cyber: "Cyber warfare could be the archetypal illustration of 'asymmetric warfare'—a struggle in which one opponent might be weak in conventional terms but is clever and agile, while the other is strong but complacent and inflexible."[42]

The exploitation of asymmetry is frequent in modern conflict, but it is difficult to assess and adapt to. An example such as insurgents "blending in" to local populations to avoid detection is illustrative of asymmetric tactics.[43] The process of blending in allows them to work from the inside out against the strategic weak point, the desire of most Western militaries to avoid civilian casualties. The same occurs in cyber, where a potential aggressor will identify and manipulate those areas of vulnerability.

What makes asymmetry such a pressing issue in cyber is what Kshetri refers to as his seventh proposition: "a higher degree of dependence on digital technologies increases a nation's vulnerability to ICT related negative asymmetry."[44] The previous section indicated that developed nations, the United States in particular, have been increasingly focused on creating cyber capabilities across all

pillars that support national security. Following Kshetri's prediction, these capabilities generate a higher degree of dependence on digital technologies and thereby increase vulnerability. As total saturation of everything from power stations to command and control warfare centers occurs, dependence on digital technologies becomes increasingly pronounced.

Rod Thornton takes this a step further when he writes that the increasing dependence on all things digital brings with it a concomitant of vulnerability.[45] Nearly all scholars agree that the cyber domain is highly asymmetric and that asymmetry is problematic. Elihu Zimet and Charles L. Barry write: "cyberspace is a tool amenable to asymmetric warfare because it can be used anonymously."[46] Jose Nazario also examines the nature of cyber hostilities, writing that it can be examined in the context of guerrilla and asymmetric theories used in conventional military conflict.[47]

Where does the vulnerability from the digital world originate? The vulnerability largely originates out of the sheer complexity of the systems on which the national security infrastructure depends for its operation across all the pillars of national security. Even when a system is well tested, an asymmetric challenges can arise in the most unexpected places, as was the case when a seventy-five-year-old Georgian grandmother cut off the Internet to Armenia with a shovel.[48] At the time of the Internet outage, Georgia and Armenia blamed Russia before the real culprit was identified.

There is no silver bullet vulnerability within the cyber infrastructure. Rather, vulnerabilities expose a dependent party to the potential for "a death by a thousand cuts."[49] These cuts can range in size and scale, and if unchecked, many can fester and become lethal.

There are multiple causes of vulnerabilities. First, software often hides zero-day exploits, which are mistakes or unintended effects written into lines of code that are difficult to find, assess, and mitigate. Zero-day exploits are best referred to as known unknowns. It is known that every software has zero-days, but it is unknown what those zero-days are. Most often these mistakes are unintentional; however, sometimes they are not. Software vendors attempt to minimize damage by rapidly patching vulnerabilities as soon as they are discovered. Second, there are interactive vulnerabilities. Because networks combine multiple different systems, they often interact in ways that could not have been predicted by the network designer. Third, there are resource vulnerabilities. As the number of systems expands, the number of qualified security personnel to monitor them does not always keep pace. Fourth, there are environmental vulnerabilities that occur with non-network environmental factors and influence network function. Examples of environmental vulnerabilities would include hurricanes, tornadoes, earthquakes, floods, and solar flares. Fifth, there are capacity vulnerabilities. Similar to resource vulnerabilities, capacity vulnerabilities are the limits at which

any given system can operate. Often attackers attack the functional capacity of a network. Sixth, there are human vulnerabilities. The most prevalent and significant vulnerability to any network is its human users. Humans are vulnerable to a wide variety of attacks, most often regarding social engineering. This is not an extensive list of the causes of vulnerabilities; rather, it is a basic grouping of the more often discussed sources of vulnerability.

Each type of vulnerability can be minimized, and the goal of any systems administrator is to minimize threats system-wide. However, as systems add on to systems, potential vulnerabilities increase. When considering asymmetry in cyber it is necessary to consider the importance of managing risk and the relationship that increasing digital dependence has on developed nations compared to potentially less developed rivals.

Increasing imbalances in the dependence of actors within the cyber domain cause asymmetry. This increased dependence is a difficult measure because it spans so many systems within and between the pillars of national security. Chapter 8 examines how intelligence organizations can weigh in and provide insight into the areas where national dependence on cyber has generated the greatest vulnerabilities. Prior to intelligence assessments it is necessary to identify a broad outline of vulnerabilities. This identification process serves as a tool by which to identify the positive and negative asymmetries for both defensive and offensive decision-making. For general comprehension of the asymmetric nature of the domain, it is possible to rely on a broad measure of digital dependence. Such a measure needs to be able to provide insight across all the pillars supporting national security.

A broad measure is necessary because asymmetry affects how decisions are made within the cyber domain. A decision-maker would have a hard time deriving a benefit from attacking a country with few to no cyber assets via cyber means. If a target's dependence on cyberspace is limited, the effect of the attack would be minimal; therefore, any resultant utility to be gained would also be minimal. Conversely, it is logical for a state with few cyber assets to engage in hostile cyber action against a highly cyber dependent state, because it need not worry about an in-kind retaliation, and it can have a much larger effect on the state with high levels of cyber dependence. As Will Goodman writes: "at the very least, cyberspace asymmetry will cause defenders to think twice before responding asymmetrically or disproportionately."[50] This does not prevent states from developing the skills and technology necessary to engage in asymmetric conflict. On the contrary, China appears to be developing the cyber skills necessary to take advantage of American negative asymmetries.[51] Asymmetry poses problems for both the use and the defense of networks in conflict largely because of a poor formulation of what asymmetry is and how states should appropriately respond to asymmetric attacks within the cyber domain.

FIGURE 2.3 Percentage of Individuals Using the Internet (2011)



Darker colors represent higher Internet use. Data from "World Telecommunication/Ict Indicators Database Online."

In addition to issues of target availability in cyberspace between states, Derek Clark and Kai Konrad illustrate the logic of asymmetry using game theory. Their model illustrates what they refer to as a weakest link argument. They state, "where an attacker wins the war if he wins on at least one front, and the defending player wins the war only if he successfully defends on all fronts."[52] This indicates that the attack surface (number of potential vulnerabilities) is an important variable in cyber conflict.

Because asymmetry is difficult to conceptualize on a broad scale decision-making basis, it is necessary to create a generic measure that can cut across the pillars supporting national security. The best generic measure of dependence on ICT comes from the International Telecom Union's (ITU) data on Internet penetration within countries. Figure 2.3 is a map representing the penetration rates of Internet use among individuals across countries, indicating a clear divide between developed and developing nations.

The percentage of individuals using the Internet is a good society-wide measure of digital dependence because it captures the influence of ICT on the aggregate country basis. This ensures that the measure does not simply focus on military or civilian infrastructures but rather gives an approximation of the dependence of national security as a whole. Because in cyber targets spread across military and civilian sectors, it is unnecessary to separate them.

The ITU's data, as a broad aggregator of state cyber dependence, are informative in a general decision-making model. Without the applicable detailed intelligence, the data provide a means to scale power calculations in cyber to more accurately represent how the inherent asymmetry present within the domain can affect distributions of power. The measure by the ITU of Internet penetration works similarly to Bueno de Mesquita's monotonic decline in power over distance. Where he finds that power declines over distance in conventional conflict, the same is not true in cyber conflict, as discussed in chapter 1. However, power does need to be scaled in accordance with its relative vulnerabilities. As this chapter highlights, cyber is immensely important to national security, and as dependence on cyber increases, so too do the number of vulnerabilities. In much the same way distance affects power in conventional conflict, increased digital dependence affects power in cyber conflict.

Internet penetration is examined in more detail in chapter 8 when a formal model for decision-making in cyberspace is examined and developed. The important takeaway is that the cyber domain extends across all the pillars of national security and therefore contains a novel set of problems differing from conventional domains. Furthermore, because distance in cyberspace is largely irrelevant, the decision to engage in hostilities must consider constraints pertinent to the cyber domain rather than attempt to fit conventional models into the cyber mold. Chapter 4 focuses more explicitly on how power is calculated for actors in cyberspace. The cyber domain is vital to the maintenance of modern national security, and its importance is the result of increased dependence. Dependence is not universal across all nations within the international system and therefore fosters a fundamentally asymmetric quality.

CHAPTER 3

The Motivation and Utility for Covert Action

> I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones.
>
> Albert Einstein

OFFENSIVE CYBER OPERATIONS (OCOs) by state actors are a new typology of covert action. The analysis below proceeds in three sections, each adding to the case that OCOs by states are a form of covert action. First, the chapter builds a rationalist argument predicated on James Fearon's "Rationalist Explanations for War."[1] By establishing a decision-making framework it is then possible to examine why and when covert actions such as OCOs are employed. In matching rich existing discussions on covert action to a decision-making framework constructed on a rationalist foundation, the lines between decision and action are drawn out. Lastly, a summarization of the motivation and utility for covert action hones in on OCO covert action. Because expected utility theory is a constitutive part of rationality, it is not necessary to delve into psychological-cognitive approaches to explain motivations for conflict. Placing OCOs within an existing literature within intelligence studies enhances an existing debate that is grounded in a historical tradition. This serves to reduce ambiguity as to the use and effect of OCOs.

Covert actions are as old as political man. The subversive manipulation of others is nothing new. It has been written about since Sun Tzu and Kautilya. People and nations have always sought the use of shadowy means to influence situations and events. Covert action has even become a staple of the state system. A dark and nefarious tool often banished to philosophical and intellectual exile, covert action is in truth an oft-used method of achieving political utility overlooked by conventional academics. Some scholars contend that for political utility to be achieved, activities such as war and diplomacy must be conducted transparently. The discussion below illustrates the shortsighted naïveté of the current conceptualization of political utility predicated largely on moral and ethical conceptualizations rather than the primacy of mathematics. Political utility is not the transparent achievement of political ends; instead it is best thought of in its original economic intent, a measure of satisfaction. Covert action is, and has always been, a tool aimed at achieving positive utility for political leaders. As with

its overt counterparts, it is not always successful; however, this lack of success does not diminish its ability in many circumstances to achieve political utility.

James Fearon states the central puzzle about wars is that they are costly but still recur.[2] When creating a rational model for any form of conflict it is necessary to root that model in a motivation for conflict, and furthermore, the result of any conflict must have a measureable utility. Below it is argued that states employ covert action against adversaries to narrow the bargaining range on issues to prevent, preempt, or minimize the extent of war. The motivation for using covert action is largely the same as that for all forms of conflict. The utility is defined in the ability to covertly alter an adversary's policy positions. Covert action, Track II diplomacy, or the silent option, as it has often been known, allows for the bridging between the security dilemma of neorealism and the complex interdependencies of neoliberalism. This creates a space in which states can use tools to extend the time constraints of international relations identified in neorealism to foster a potential for the absolute gains associated with neoliberalism. At its most basic, the covert alteration of the bargaining range extends the time horizon outward and makes possible interactions of neoliberalism due to a reduction of information problems.

SETTING THE BASIC ASSUMPTIONS

Before diving into the motivation and rationality for conflict, it is helpful to establish the basic assumptions contained below. First, rationality within is reflective of bounded rationality, which is used to more accurately reflect the conditions present within the international system. Herbert Simon serves as a guide in isolating what rationality means in this context: "To deduce the procedurally or boundedly rational choice in a situation, we must know the choosing organism's goals, the information and conceptualization it has of the situation, and its abilities to draw inferences from the information it possesses. We need know nothing about the objective situation in which the organism finds itself, except insofar as that situation influences the subjective representation."[3]

Second, there are times when it is possible that a national leader might act out of self-interest rather than in the national interest. Covert action conducted by a state may have positive utility for an individual of a state and may at the same time be irrational because it has a negative utility for the state. Such an instance would indicate engaging in covert action would be irrational from a national security perspective. Leaders might act based on their individual rationality and still force their state to behave irrationally. Hitler would be a prime example of this in his inability to fully assess the calculus of war against multiple powers, particularly a resource-rich Soviet Union and United States. While rationality has many fallibilities, here it is necessary to assume states act as unified rational

actors in the national interest. This assumption establishes a parsimonious explanation for the use of certain tools of state, specifically covert action.

THE MOTIVATION AND RATIONALITY FOR CONFLICT

Fearon cites three commonly held rationalist arguments for why states are willing to engage in conflict despite knowing they are forgoing the lesser ex-ante costs of bargaining in favor of higher ex-post costs associated with conflict. Anarchy, preventative war, and positive expected utility have substantial literatures behind them.[4] Each in some way develops a logic for casus belli. Waltz, Mearsheimer, and other neorealists state that the security conundrum makes conflict inevitable because there is nothing within the international anarchic order that prevents states from engaging one another in hostilities. Fearon notes that while this is true, the lack of constraints on war occurring and the fact that wars occur does not present sufficient grounds for rational conflict. He illustrates that despite a lack of constraints preventing war, the act of engaging in war is almost always ex-post inefficient and therefore irrational. Furthermore, he cites realist arguments that states engage in preventative wars as a rational act. Although realists argue it is rational to engage in a war in the present to minimize future costs, Fearon illustrates that this is a flawed logic. Ex-post inefficiencies are still present in both anarchic and preventative war, which according to Fearon makes them both irrational.

In this argument Fearon only briefly touches on what the real logic behind these causes of war indicates. They, in and of themselves, are not motivations or rational explanations for war; rather, they are structural constraints that make war more likely. It is these structural constraints on the international system that facilitate those motivations forming the basis for the rational instigation of conflict.

Lastly, Fearon indicates that establishing a foundation for conflict predicated on a positive expected utility for conflict is also irrational.[5] He largely bases this on a critique of Bruce Bueno de Mesquita's argument that states will not engage in conflict if they do not have a positive expected utility.[6] However, Bueno de Mesquita is not arguing that states should go to war if they have a positive expected utility, only that it is rational if they do decide to go to war.[7] Nor does Bueno de Mesquita claim that both states need to have a positive utility to engage in conflict; rather, he finds that only the conflict initiator must have a positive utility. He specifically does not indicate that both parties to a conflict need to find it rational, because this would be a violation of Arrow's impossibility theorem.[8] Reality indicates that it is possible for two states to both expect positive utility from conflict with one another; this would constitute a rational miscalculation of subjective probabilities.

Because the expected utility of international conflict is only one possible option in a range of policy options, its utility must be weighed against other options such as diplomacy. This creates an intrapersonal comparison of utilities, meaning that utilities are comparable across decisions within a single individual (state). This differs from assumed utility construction, in which decisions are identical across individuals (states), or interpersonal utility construction. The subjective nature of utilities in a bounded sense of rationality makes interpersonal utility comparisons illogical.

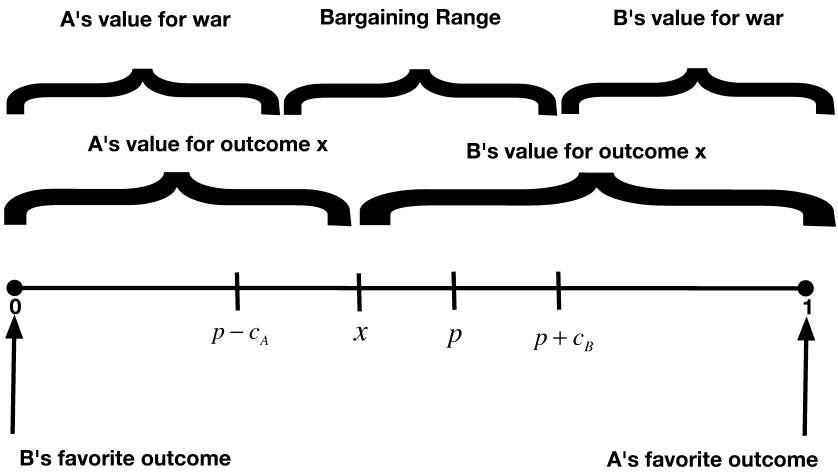
Utilities help facilitate preference ordering through intrapersonal comparison of subjective utilities. This intrapersonal comparison indicates that if state A has a positive utility of .08 for conflict and a positive utility of .09 for covert action, covert action is likely to be ranked higher based on a cardinal preference ordering of utilities. The utilities are not intrapersonally independent. This is an important distinction that needs to be made in rationalist explanations of war. While the first two explanations as posited by Fearon are clearly predicated on weak rational explanations (because they are not causal explanations but structural frameworks), the third is not a causal explanation and more accurately underpins all aspects of rationality as indicated by Simon.

Both Fearon and Bueno de Mesquita make the argument for the bounded rationality of actors. Within a bounded rationality model, the utility for conflict must be positive for a state to rationally engage in hostilities. Bueno de Mesquita does not explain why states go to war, only that the act of going to war with the conditions he presents is rational. The greater the utility, the more compelling the argument for conflict. He writes: "Being rational simply implies that the decision maker uses a maximizing strategy in calculating how best to achieve his goals"[9] This is a clear indication that rationality in Bueno de Mesquita's conceptualization is simply a way of ranking utilities to achieve the best result.

Claiming that rationality is predicated on a full understanding of the utility for conflict both ex-ante and ex-post, Fearon asserts that the motivation for conflict is largely based in three root causes. First, war can occur due to private information and incentives to misrepresent.[10] Second, war can occur due to commitment problems between states.[11] Third, war can occur due to issue indivisibilities.[12] These are three situations in which it is not possible to negotiate an ex-ante settlement to avoid hostilities within Fearon's bargaining range of possible ex-ante solutions.

Figure 3.1 is Fearon's illustration of the bargaining range in which states are either unwilling or unable to maintain a commitment or attempt to conceal or misrepresent information. The bargaining range below is the space between $p - c_A$ and $p + c_B$. It is not in dispute that in many if not all instances there exists an ex-ante bargaining range. Nor should it be believed that Bueno de Mesquita's

FIGURE 3.1 Fearon's Bargaining Range



From Fearon, "Rationalist Explanations for War."

expected utility theory of international conflict precludes such a bargaining range and provides a direct path to conflict.

If such a range were available, it could possibly be subsumed within Bueno de Mesquita's model in the mathematical notation of changes in policy positions over time by $\Delta(U_{ii} - U_{ij})_{t0 \to t+n}$ for the conflict initiator and $\Delta(U_{ij} - U_{ii})_{t0 \to t+n}$ for the defensive party.[13] The causes Fearon identifies as the locus for casus belli—indivisibilities, misrepresentation and miscalculation, and commitment problems—are viable characteristics that can be incorporated into a construction of utility. Even if these are not adequately assumed into the mathematical notation, it is logical to assume that each alternative option available to a policy-maker also carries with it a unique expected utility function. These utilities are then intrapersonally comparable.

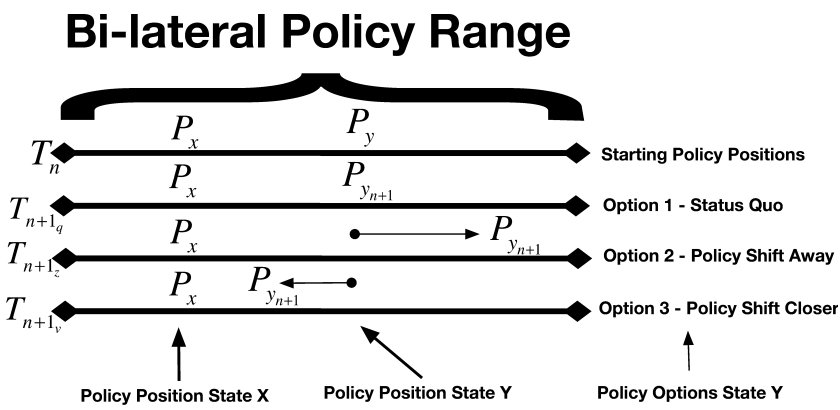
Based on Fearon's bargaining range there are three instances in which international conflict can be initiated rationally: (1) rational miscalculation due to a lack of information or a disagreement about relative power due to information asymmetries, (2) issue indivisibilities, and (3) commitment problems. Each of these rationalist explanations for war is, however, predicated on the conflict initiator having a positive expected utility. Rarely if ever has there been a case in which two states have mutually declared to engage in hostilities at the same time against one another. Most if not all conflict has a conflict initiator. The definition of conflict initiator can at times be blurred, yet it has never been the case that two states mutually agreed to settle their differences by engaging in warfare without one having fired the first shot.

Motivation and utility should be separated when discussing conflict. While in realism the world is black and white, us and them, the complex interdependencies of neoliberalism offer a hybrid model for conceptualizing how states interact. Although Fearon claims to be making an argument in support of realist "rational" explanations for war, he is in fact making a neoliberal argument that allows for the mitigation of temporally constrained relations. The information sharing necessary to avoid war is the product of interactions and therefore requires time to materialize. Information problems are most acute and therefore in a conditionally rational environment most prone to occur when the time horizon is short. His argument establishes states that are not defined solely by individual zero-sum interactions, but rather by two competing measures of expected utility, the ex-ante and the ex-post, and in so doing he extends the horizon of the future outward. Thus, the bargaining range represents what Arthur Stein refers to as coordination and collaboration.[14] Stein writes: "Regimes arise because actors forgo independent decision-making in order to deal with dilemmas of common interests and common aversions. They do so in their own self-interest, for in both cases, jointly accessible outcomes are preferable to those that are or might be reached independently."[15]

There is no mechanism within traditional neorealist literature by which states can achieve a bargaining stance ex-ante. Instead the victor imposes his demands on the loser following the conclusion of hostilities, as a requirement for concluding hostilities, or as a requirement for avoiding hostilities. Both sides are caught in a prisoner's dilemma and are willing to defect, creating an irrational (inefficient) ex-post result. What Fearon illustrates is a situation in which states can create a mutually established agreement, a regime that seeks efficiency. His argument is in line with Bueno de Mesquita's necessity for a positive expected utility. When an alternative policy option to conflict arises, it is necessarily compared to Bueno de Mesquita's concept of expected utility for international conflict. If the alternative course of action offers a higher utility, that option would be the rational choice. If options with greater political utility exist, these options should alter the expected benefits to be gained by conflict and alter the utility of conflict, creating a diminishing utility for conflict over time.

If a state has a negative utility for conflict, then, engaging in conflict would be irrational. Therefore it is possible to have multiple outcomes of the decision process. A state can find it rational to engage in conflict yet have other preferences providing greater utility. Conflict could provide the greatest utility and therefore be chosen as the maximizing preference. Or conflict could have a negative utility. In the final instance, choosing conflict would be irrational regardless of the structural constraints of the system. In such an instance it would be more logical for a state to seek out an alternative to conflict. Every option has a measure of utility to the decision-maker (the unitary actor). Having utility does not

FIGURE 3.2 Bilateral State Policy Interaction Possibilities



equate to choosing a preference unless that preference provides a utility maximization for the actor.

While the logic is complex, it serves to establish that there are three instances in which conflict is rational, and there is a mathematical means of assessing when it is rational to engage in conflict within these instances (expected utility theory). The establishment of rationality behind conflict has thus far failed to sufficiently identify a motivation for conflict. Simply stating that there are issue indivisibilities is not a sufficient motivation for conflict; likewise, information asymmetries and commitment problems also do not provide a motivation for conflict. They instead describe the characteristics in which conflict can occur.

A policy range in which states interact defines the bargaining range for states. Returning to the policy range illustrated in chapter 1, Figure 3.2 establishes the bilateral policy range between two states. Broadly stated international relations are the process by which states influence one another's policies. The bilateral policy range is a relationship of policies between two states. It is in this policy range that the rational explanations for conflict can occur. Here the specific focus is on the bilateral policy range of states because although covert action occurs with multiple parties to a given action, the component capabilities are not conducive to an additive function. When two states jointly develop code, they are left with one program, not two. When two states combine conventional armed forces such as tanks or soldiers, each additional tank or soldier adds to the capability of the whole. Although the potential outcome capability of a cyber weapon might be greater, the effect that weapon achieves is measured singularly. More simply, mathematically there is no adequate way to distinguish combined cyber capabilities. Likewise, once a capability has been developed, that capability is equally capable for each party to a given action. The same is not true of com-

bined conventional arms. If prior to the use of a cyber weapon system one party were to abstain, the other party could continue the operation without a relative loss of capability. Thus, for the purposes of utility construction the initiation of OCO at the point of initiation is best characterized by a bilateral rather than a multilateral policy range.

At time T_n two states are aligned on a policy spectrum, and the distance between them represents the difference between their respective policy positions. The more proximate the states are, the closer their policy positions. Likewise, the further they are apart, the more they diverge in their policy positions. Assuming state P_x is the potential conflict initiator, it looks for movement in the policy position of state P_y. State P_y has three options: (1) it can maintain the status quo, (2) it can move its policy further away from P_x, or (3) it can move its policies more in line with P_x. In this situation state P_x will likely view a policy shift away from its position as an act of aggression; it might also view the maintenance of the status quo as an act of aggression. Lastly, it might view the policy shift of state P_y as occurring too slowly, which could also be construed as a hostile act. In each of these instances there is a possibility for the potential conflict initiator to view the actions by its adversary as hostile. Option three is least likely to be viewed as hostile, while option two is most likely to be viewed as hostile, with option one somewhere in between.

The motivation for any conflict is rooted in the policy divergences between nations on issues. Neoliberalism and Fearon's claims for rationality both indicate that in most instances there is a workable settlement, which can result in a more efficient outcome than conflict. Before resorting to an all-out conflict and working within Fearon's identifiable areas, preventing an ex-ante settlement is another set of options open to policy-makers that has been used for millennia in an effort to mitigate the rationalist explanations for war and provide a mechanism for facilitating an ex-ante settlement.

Covert action steps into the breach short of overt armed conflict between two belligerents. Covert action can occur throughout the policy interactions of states. Covert action serves as a tool for the mitigation of information asymmetries, issue indivisibilities, and commitment problems. It can serve as a tool to improve the bargaining position of a state or to bring states back to the bargaining table.

POLITICAL UTILITY AND THE LITERATURE

For a discussion on development of political utility for covert action to move forward directly from above to an examination of the need for covert action, it is important to define political utility. If covert action is truly a third option, then there is a need to express its utility in the context of the ex-ante and ex-post costs.

Peter Fishburn writes of utility theory: "On the practical level, utility theory is concerned with people's choices and decisions. It is concerned also with people's preferences and with judgments of preferability, worth, value, goodness or any number of similar concepts."[16]

Yet in extending utility from the individual to the state we arrive at the concept of "political utility." Disaggregating the terms "political" and "utility" helps to codify their meaning in the context of a decision-making model for state actions. The first term, "politics," is derived from the Greek term *politika* examined in detail by such philosophers as Aristotle and Sun Tzu. The term "politics" is of little help in understanding the term "political utility." Politics simply refers to the "art or science of government."[17] "Utility," in contrast to politics, is a powerful economic concept developed in exhaustive detail and honed into its modern form by Jon Von Neumann and Oscar Morgenstern.[18] The economic concept of utility was first carried over to political science in the 1950s with the work of Anthony Downs.[19]

Downs states that utility is simply a "measure of benefits."[20] He follows directly in the footsteps of Oscar Von Neumann and John Morgenstern and defines utility by stating that a rational individual, given a series of alternatives, will weigh the values of each and create a *complete* and *transitive* preference ordering. The individual will then choose the preference with the highest value. The economic terminology associated with utility is not related to both sides understanding the preference orderings of the other. Rather, it is an individual decision-making process. Therefore, the utility of two individuals in the same situation can differ dramatically. This is essentially what Downs meant when he wrote that a voter will act toward "his own greatest benefit."[21] If all voters had the same utility calculus, there would be little need for elections. To create political utility we aggregate the two terms: the art or science of government and the measure of benefits. Political utility is the measurement of the benefits accrued to government in a unitary state-centric system.

The concept of the benefits to government is not as straightforward as it might at first glance appear. Here it is assumed that the government is a representative of the collective will or interest of the people. This might not be true in nonrepresentative systems, yet as individuals within these systems must respond to their government, it is possible by extension to assume a diffusion of collective benefits or costs associated with a government's actions. These benefits and costs are not always distributed equally among the citizens of a nation. However, often in policy areas such as national defense they are assumed to comprise common pool resources. Whether the motivation for an action originates internally or externally, the utility scores are calculated based on what can be gained or lost in relation to the opponent. National gain or loss differs significantly from what might be gained or lost politically within a nation. An

argument predicated on domestic political utility development functions separately from the argument being posed in relation to state-on-state covert action in this present chapter.

Political utility is not perfect and contains many failings. Many of these failings are found in the inability to aggregate individual preference orderings, cognitive failings as examined by Amos Tversky and Daniel Kahneman, or even in-group dynamics illustrated by Irving Janis.[22] Despite its limitations, rational choices must be conditional upon an opposing party's simultaneous choice. Robert Grafstein notes "Conditional expected utility maximizers are concerned with expected utility, whether or not they caused it."[23] Rational decisions are reached independently of one another in most instances. Covert action has political utility because it seeks to maximize the benefits to a government and by extension its people in the same way as overt diplomatic bargaining and overt military conflict.

THE USE OF COVERT ACTION FOR POLITICAL UTILITY

The National Security Act defines covert action as "[a]n activity or 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."[24] Covert action goes by many names, often referred to as Track-II, the quiet option, or the third option.[25] In an international system where the formal declaration of war is becoming an increasing rarity, the gap between diplomatic and overt military dispute resolution has never been wider.

Into the gap between diplomatic and military dispute resolution states leverage a wide array of tools; among these is covert action, and within covert action is a subset of actions referred to in joint publications as cyber operations. Covert action is not a rare occurrence. Gregory Treverton identified more than nine hundred operations of various levels between 1951 and 1975 in which the "silent option" was used.[26] Loch Johnson indicated that covert action was used very differently by each presidential administration.[27] Not only do the aggregate number of covert actions vary from president to president, but the intensity of those actions varies as well. More recently the administration of President Obama has sanctioned the use of at least 239 covert drone strikes in Pakistan as of late 2012.[28] And while the silent option appears to be not so silent and frequently used at times, the question still remains: Why do we use covert action?

Loch Johnson's quote from Henry Kissinger provides a succinct logic for covert action. According to Kissinger: "We need an intelligence community that, in certain complicated situations, can defend the American national interest in the gray areas where military operations are not suitable and diplomacy cannot

operate."[29] As was stated above in regard to Fearon's bargaining range, there is quite frequently a middle area in which bargaining simply becomes too difficult. It is this middle area that Kissinger refers to as the "grey area." It is an important point to belabor because it provides nuance to the concept of covert action. By parsing out what covert action is, it is possible to contextualize modern covert acts. Below are a series of quotes from practitioners and scholars alike. Each helps to frame the rationale for covert action and to define its broader boundaries. The quotes often provide contradictory frameworks within which to understand covert action.

Practitioner Duane Clarridge writes in his memoir: "Covert action entails special activities, such as political action and paramilitary operations, to advance U.S. foreign policy objectives by influencing events in foreign countries. I believe I concluded at this time that my purpose in life and the reason I was in the CIA was to advance the interests of the U.S. government and the American people abroad."[30]

Practitioner James M. Olson writes in his book on the morality of spying: "Espionage is a crime in every country, and the United States practices it in almost every country. Covert action, defined as intervening secretly in the affairs of foreign countries, is a blatant violation of international law."[31]

Practitioner Theodore Shackley writes in his memoir: "Covert action operations can be as deceptively peaceful as a letter-writing campaign or as flagrantly violent as a guerrilla uprising. In every case, though, the instigating government must make at least a token effort to hide its hand."[32]

Loch Johnson quotes Les Aspin as saying: "covert actions should be as consistent as possible with the moral character of the American public, so that if some action becomes public, it would not be terribly embarrassing to the government of the United States because it is not something most Americans would consider immoral."[33]

President Richard M. Nixon writes: "Overt economic or military aid is sometimes enough to achieve our goals. Only a direct military intervention can do so in others. But between the two lies a vast area where the United States must be able to undertake covert actions. Without this capability, we will be unable to protect important U.S. interests."[34]

Each of the above quotes offers a perspective on the value of covert action ranging from the practical, moral, and legal. While each varies on the moral and legal ramifications of covert action, each to some extent acknowledges that covert action fills a necessary gap in foreign policy. Knowing there is a gray area of operations, and knowing these operations occur at varying levels, still leaves the gap of defining what constitutes covert action.

Defining covert action is less difficult than assigning its value. To define covert action it is best to establish an analytically rigorous framework. Loch John-

son outlines four broad categories of covert action: propaganda, political covert action, economic covert action, and military covert action. Each of the titles is somewhat self-evident. Johnson then takes it a step further and identifies a scale or ladder of covert action. Figure 3.3 is a modified version of Johnson's scale of covert action. The changes made to his original ladder include critical infrastructure destruction, pinpointed digital actions against combatants, critical infrastructure degradation/denial, and cyber exploitation. Each of these additions adds a host of potential actions emanating from cyber domain and falls distinctly within the ladder at various locations.

Utility is not determined by the type of covert action; rather, it is ascertained by the expected effect a covert action might have on the intended target in relationship to the possible costs associated with failure. Therefore, the further up the ladder of covert action a nation proceeds, the greater the ramifications for failure and conversely the potential for great gain. A national leader with commitment problems is unlikely to be assuaged by covert actions on the lower thresholds. However, the consequences of an extreme covert action such as a failed state-sponsored coup d'état could lead to overt war and a great deal of negative utility. Covert actions must be tailored to meet the needs and risks of a given situation. Lower thresholds likely pose less risk than higher thresholds of action. They are also likely to offer less reward. Yet, because utility can be intrapersonally additive in many instances, a series of actions with little independent political utility might be more effective and result in a combined utility greater than a single risky operation with a one-time possibility for a higher utility payoff.

The threshold of covert action(s), as in any diplomatic or military setting, must be targeted to achieve the greatest benefit with the lowest cost. Temporal problems aside, in attempting to bridge the gap there are many tools that can attempt to fill the bargaining range among which covert action is one typology. Overt forms of signaling include threats or the imposition of economic sanctions.

The motivation and utility for conflict are those variable factors that lead states to engage in hostilities in the first place rather than negotiate. Although there are many theories analyzing the motivations for conflict ranging from misperceptions to outright irrationality, this book argues the reality behind the motivation for most major state-on-state wars, and the utility assigned to those wars occurs because of an information gap between the potential belligerents. Furthermore, this information gap can be and has been altered by covert actions of states. Because covert action can fill the gap between war and diplomacy, it can achieve political utility.

Positive utility through covert action occurs when narrowing the range of policy options minimizes issue indivisibilities and concealed information, or by changing the leadership of an opponent state. Below are several examples,

FIGURE 3.3 Covert Action Ladder

Threshold Four: Extreme Options	
34	Use of WMD
33	Major secret wars
32	Critical infrastructure destruction
31	Assassination
30	Small-scale coup d'état
29	Major economic dislocations; crop, livestock destruction
28	Environmental alternatives
27	Pinpointed covert retaliations against noncombatants
26	Torture to gain compliance for a political deal
25	Extraordinary rendition for bartering
24	Major hostage rescue attempts
23	Pinpointed digital actions against foreign combatants (noncivilians)
22	Sophisticated arm supplies
Threshold Three: High-Risk Options	
21	Massive increases of funding in democracies
20	Critical infrastructure degradation/denial
19	Small-scale hostage rescue attempt
18	Training of foreign military forces for war
17	Limited arms supplies for offensive purposes
16	Limited arms supplies for balancing purposes
15	Economic disruption without loss of life
14	Information communications systems disruption without loss of life
13	Modest funding in democracies
12	Massive increases of funding in autocracies
11	Large increases of funding in autocracies
10	Disinformation against democratic regimes
9	Disinformation against autocratic regimes
8	Truthful but contentious propaganda in democracies
7	Truthful but contentious propaganda in autocracies
Threshold Two: Modest Intrusions	
6	Low-level funding of friendly groups
5	Cyber exploitation
4	Truthful, benign propaganda in democracies
Threshold One: Routine Operations	
3	Truthful, benign propaganda in autocracies
2	Recruitment of covert action assets
1	Support for routine sharing of intelligence

Source: Johnson, "Secret Agencies," 41.

examined in brief, of the use of covert action to achieve positive political utility in the gap between public diplomacy and outright war. Starting with an action with little to no relation to cyberspace facilitates a discussion, as capabilities are developed to leverage a new domain for action. Covert actions fill in that grey area where it is necessary to find solutions that do not fit within diplomacy or overt conflict. Each case is designed to illustrate actions within this gap.

AFGHANISTAN 1980s

(a) Milt Bearden, the CIA chief of station in Islamabad during part of the 1980s, worked extensively on providing weapons to indigenous fighters in Afghanistan.[35] The program popularized in such films as *Wilson's War* and others was a strategic opportunity to slip between the overt ends of the foreign policy spectrum. Afghanistan operations also received broad congressional support, a rarity for covert action.

(b) By providing weapons indirectly to the Mujahedeen fighters, the CIA was able to place pressure on the Soviet military without having to commit any American boots on the ground and without having to make political concessions. While the origin of the weapons was less than secret, it was still covert and plausibly deniable. With the increasing power of the weapons, which eventually included Stinger anti-aircraft missiles, the CIA gave the enemy of its enemy the tools to make life increasingly difficult for Soviet soldiers and airmen. The Soviets lost thousands of soldiers and spent enormous sums of money, all of which helped to weaken their strategic position globally, reduce information asymmetries, and increase commitment problems as the regime began to crumble in the late 1980s.

(c) The covert deployment of weapons provided political utility by increasing the pressure on an adversary and by forcing them to recognize geopolitical and strategic limitations. The ex-post costs of the weapons program were significantly less than the costs associated with an overt war, and the results created benefits far greater, and did so more efficiently, than did the comparable diplomatic efforts. The morality of the endeavor has been questioned more than twenty years later, when many of the same fighters to whom the CIA provided weapons are now directing their animosity against the United States, yet for a period of approximately twenty-five years the cost-to-benefit ratio provides an example of one of the best covert operations ever run.

ESTONIA 2007

Unlike Afghanistan, Estonia was not engaged in conflict with another nation, but rather it was shifting away from its opponent on the bilateral policy spec-

trum on very specific issues with ideological associations. Guns and missiles provided to Russian minorities in Estonia would have been overkill and would likely have achieved a collective NATO Article 5 response. Direct complicity in an ideological debate would have undermined the image of a strong and worldly Russia; however, a collective action by Russian minorities in Estonia and abroad would signal the policies of Estonia were hitting a raw nerve.

Cyber conflict complicates traditional notions of covert action largely because although computers are logical, the motivations of their users are not. Bits and bytes when used as a tool of state become messy, as was the case when the Estonian government decided to remove a Russian war memorial from central Tallinn in 2007. The move engendered a great deal of animosity among ethnic Russians in Estonia as well as within the Russian Federation. The response to the move was a large-scale distributed denial-of-service (DDoS) attack conducted against key governmental, financial, and press targets within the former Soviet republic.[36] The action itself, while not covert as it was immediately visible to the Estonians and the world, was consistent with covert action. Most reports indicate that the attacks were sanctioned by the SVR, the modern version of the First Chief Directorate of the KGB.[37] The attacks, although not conducted by the SVR, were likely coordinated by or facilitated through official channels.[38] The covert aspect is not the resultant action; although the initial phases of the attack planning and implementation were conducted covertly, the covert nature of the operation is that it obscures responsibility and allows for extreme policy dissatisfaction to be made known without either overt diplomacy or military action.

The overall consequence of the attacks against Estonia was severe in the short term but mild over the long haul. This type of operation is classified on the ladder of covert action in the third threshold as a combination economic action without loss of life and information communications systems disruption without loss of life. The attack falls under these two categories within the third threshold because of the breadth of the attack spanned across financial, media, and governmental organizations. If the attack had been solely directed at one type of institution, it would have been more easily classifiable.

This type of action is covert because it achieves a political statement without directly implicating a national sponsor. Through cyberspace the Russian Federation was able to make a significant political point without losing face through overt diplomacy. Thus, while the action was visible, the culprits were not, making it covert. The political utility of the act lies in the ability to convey a significant foreign policy message without attribution from the sender. More simply, the result was a signal: "we can do significant damage to your information and economic infrastructure if you engage in policy behaviors we deem hostile." Such a signal increases political clout and can increase uncertainty of an opponent within the bargaining range of issues.

The long-term consequences of the action seem to have run antithetical to its original goals. Instead of shifting the policies more in line with Russian and Russian minority interests, the action appears to have instead pushed the Estonians much more quickly into complete integration with Europe and NATO. Moreover, the actions gave impetus to the rush for NATO to address issues associated with cyberspace, including the establishment of the NATO Cooperative Cyber Defense Centre of Excellence in 2008 and a cyber pledge for mutual defense under Article 5 of the NATO treaty in 2014.

SYRIA 2007

The cyber attacks against Estonia were exclusive to cyberspace. Although the effects were felt by citizens across the country, there were no resultant kinetic effects reported. Cyber operations have several ways of facilitating or generating kinetic (noncyber domain effects). Outside of the movies, where cyber operations can directly affect kinetic violence, the more common way that a cyber operation affects kinetic changes is by acting as a force multiplier for kinetic weapon systems. A September 2007 attack against Syrian nuclear facilities serves as one of the best documented examples of a covert OCO facilitating kinetic destruction. The attack occurred when Israeli jets invaded Syrian airspace undetected and bombed what the CIA later disclosed was a nuclear facility being developed jointly by the North Koreans and the Syrians.[39] This attack was a coordinated conventional military attack made possible by covert cyber actions. The Israelis, as Richard A. Clarke and Robert K. Knake indicate, used cyber means to spoof Syrian air defense mechanisms.[40]

This type of attack is a dual covert-overt attack. Once the bombs were dropped, the attribution and covert nature of the attack was eliminated. However, the ability to conduct the attack was predicated on the covert operation that shifted the tactical advantages wholly in favor of the Israelis. To accomplish the takedown of Syrian air defenses, the planning and implementation of cyber weapon systems likely took months to achieve a small window of opportunity.

Does this type of attack fit within the bargaining range above as defined by Fearon? Not quite, but the political utility associated with such a covert operation is plainly obvious. It is possible to claim that the combined attack eliminated an indivisible issue, the Syrian development of nuclear capabilities. Regardless of whether the attack falls within the bargaining range where covert action is most effective, it was both ex-ante and ex-post efficient from the Israeli perspective. They were able to eliminate a potential threat with minimal casualties. By eliminating the nuclear facility, the Israelis forced Syria toward a more favorable policy position indicating a positive utility.

STUXNET 2009

In 2010 Iran admitted experiencing problems with their nuclear enrichment facilities at Nantaz. The *Wall Street Journal* then reported that Iran was the victim of a highly sophisticated cyber attack.[41] Dubbed Stuxnet by the Belarussian computer security firm VirusBlokAda,[42] the program was sanctioned by President Obama as part of a top-secret operation called Olympic Games. Following the initial release of information by VirusBlokAda and the *Wall Street Journal*, other news organizations followed up with stories claiming that the malicious software specifically targeted Siemens systems in configurations typically used for centrifuges designed to enrich uranium. The result was a delay of between one and three years in the production capabilities of highly enriched uranium (HEU).[43] Software security agency Symantec followed up on the Stuxnet story by issuing a report detailing the malicious software.[44] Combined, these news reports and corporate analyses of the software provide the starting point of a unique picture of one of the first significant cyber covert actions with acknowledged kinetic effects.

While other chapters detail that the software was designed to be very specific in its attack protocol, of relevance to this chapter is the political utility of such an attack. To understand the political utility of the attack it is necessary to contextualize the situation. Iran had for years vehemently denied it was working toward producing nuclear weapons capabilities.[45] It had consistently claimed it was working on nuclear production solely for peaceful purposes and had on numerous occasions invited International Atomic Energy Agency (IAEA) inspectors to participate in limited inspections. Iran had also begun reporting on its nuclear programs in line with requirements by the Non-Proliferation Treaty (NPT). However, the Iranians would not allow inspectors from the IAEA into certain key facilities, making their self-reports and the entire verification process suspect to claims against its accuracy.[46] The lack of transparency present in Iranian nuclear facilities created an information asymmetry between Iran and its primary accusers, Israel and the United States. The situation increased in importance with heightened rhetoric by Iranian president Mahmoud Ahmadinejad, who on numerous occasions called for the destruction of Israel. Ahmadinejad's rhetoric led to worries that a potential nuclear weapon developed by Iran could be directed against Israel.

Diplomatic efforts were stalled, and long-term engagement in a counterinsurgency campaign by the United States in Iraq made the possibility of an overt war against Iran highly unattractive. The objective OCO against Iran became twofold: reduce information asymmetries between Iran and the world by exposing an enrichment process that exceeded normal civilian use, and delay the eventual production of a nuclear weapon by hindering the enrichment pro-

cess. The situation presented to U.S. and Israeli decision-makers fell between both ends of the overt spectrum and provided a middle range within which to achieve two political objectives.

The Stuxnet worm was able to provide political utility by first illustrating that Iran was enriching uranium beyond civilian use. This information transparency paved the way for enhanced sanctioning efforts on the international level and opened up new diplomatic alternatives. These diplomatic alternatives were only feasible because of the second aspect of Stuxnet, time. If the covert operation had only identified Iran's movement toward HEU, then it would have increased the need for overt armed conflict. However, because Stuxnet delayed the production of HEU,[47] it provided time for overt diplomacy to work as an alternative to other forms of power and thus reduced the immediate the need for conflict. The logic for this argument is well documented in President Obama's authorization of the Olympic Games program, of which Stuxnet was a part. David Sanger of the *New York Times*, reporting information gained from administration sources, wrote: "If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region."[48]

The operation was not perfect. The version of Stuxnet that blew the lid on the operation did not have a self-delete function and was eventually released into the wild. Although it did not have significant adverse effects on other systems due to its programing structure, it would have been of greater benefit if the operation had remained completely secret.[49] The loss of anonymity in the long term associated with the revelations of the attack instigators by David Sanger, who cited "Top Officials," has not had significant adverse effects as the processes for mitigating the potential for overt acts of warfare were already well underway.[50] As illustrated in subsequent chapters, this particular covert action was conducted by two nations with a significant power advantage over their adversary.

OPERATION CLEAVER

Beginning in 2012 Iranian actors engaged in an increasingly sophisticated series of attacks against U.S. and allied interests.[51] The attack, first publicly reported by the *Wall Street Journal* in September 2013, included fifty different targets in sixteen different countries.[52] One of the more significant targets was the NMCI (Navy Marine Corps Intranet) in San Diego.[53] Other targets included aspects of the defense industrial base, critical infrastructure, universities, airlines, and hospitals. Although Cylance, the computer security company that wrote the primary forensic analysis report on the attacks, doesn't think the attacks rise to a level of significance comparable to Stuxnet, they note that the variety of

techniques, tactics, and procedures used were able to achieve substantial damage.[54] Although the hacks did not successfully compromise Industrial Control Systems (ICS) or supervisory control and data acquisition systems (SCADA), the reports indicate that the hackers were able to exfiltrate significant amounts of sensitive information.

The attacks are interesting for several reasons and are included here as an example of covert action, because over a multiyear period these attacks have had success against a large, diverse target set and are thought to be in retaliation for actions conducted by the United States and its allies. The attacks are some of the most successful attacks against U.S. interests by a nation-state other than China or Russia and indicate an increased threat posed to U.S. national security by an increasing number of state actors. In December 2014, Reuters indicated that the Federal Bureau of Investigation considered this to be a serious incident and provided information to government agencies and industry on how to protect against Operation Cleaver hacks.[55] Also of interest are the targets of the attack. Unlike criminal attacks designed primarily to steal personally identifiable information (PII) for commoditization, these attacks attempted to steal PII to establish deeper access within target systems.[56]

Although the attacks could be constitutive of cyber exploitation (CE), the aggregate result is a cyber attack (CA). More than simply removing data from the systems, the hackers engaged in manipulation of systems and infrastructure in some of the targets. Because the hackers have gained a strong foothold, Cylance indicates that these attacks establish the possibility for potential future physical ramifications able to compromise the integrity and reliability of some of the "world's most critical environments."[57] Cylance notes that the goals and objectives of the attacks are unknown, and although they are speculated as retaliation for U.S. operations, the absence of knowledge about the goals and objectives makes a comprehensive understanding of the attack unavailable. The TTPs of the hackers make it possible to identify certain actors based on skill and behavior, but the ability to halt these actors has so far been limited. This indicates that the actors have been able to achieve significant benefits with minimal risk.

THE UTILITY OF COVERT ACTION

Political utility and covert action are not mutually exclusive, nor do both sides to a dispute need to be aware of the other's actions for one side to gain or lose in political utility. For too long scholars have focused on the overt world of political utility and ignored the bargaining range affected by actions in the shadows of international relations. The above analysis seeks to remedy this by citing a broad range of literature and by bringing in statements from scholars, politicians, and practitioners alike. The analysis presents evidence that covert action can be ex-

amined using expected utility theory. Covert action is a tool of rational states. While leaders can abuse this tool, the argument set forth highlights the mechanism by which states, acting as unitary actors, can determine the utility of covert actions, whether they are conventional or cyber covert acts. Furthermore, the analysis illustrates that covert action works best in what James Fearon defined as the bargaining range between states.

Covert action so often falls to the sidelines of international relations because of its moral and ethical considerations. Additionally, the inability to gather current evidence on the state of covert action dissuades academics from engaging in a rigorous study of it and its implications. Although the gap between overt diplomacy and overt war can be large, to turn our eyes away from this bargaining range is to ignore the real-world tools being used to affect it. Covert action can and does play a role in the space between diplomacy and war. The utility of covert action is derived from its ability to alter the policy relationships of states in international relations and achieve tangible benefits to a government. Most importantly the discussion establishes that offensive cyber operations are most akin to conventional covert actions based on their need to occur in the shadows between overt diplomacy and war. By establishing that most state-on-state cyber operations are akin to covert operations or espionage more broadly, we can better develop a rational choice framework in which to understand the use of offensive cyber operations against other states. If we were to only conceive of cyber operations as an overt tool, we would severely limit their use and overlook most state uses of cyber over the last fifteen years.

CHAPTER 4

Digital Power

> I hope our wisdom will grow with our power, and teach us that the less we use our power the greater it will be.
>
> Thomas Jefferson

THE ABILITY TO INFLUENCE, "power," is a fundamental concept that underpins international relations theory. Whether approaching the world from a realist, liberal, constructivist, Marxist, or feminist perspective, chances are power plays a role in influencing state actions or the actions of individuals. Yet, for all its significance within the field, the study of power has been largely absent from many discussions on cyberspace. Below is an exploration of traditional formulations of power at the national level and examinations of the failures of these traditional notions to incorporate the value of cyber; it adds to the relevant literature by framing a debate conceptualizing power in cyberspace. To understand power in cyberspace it is necessary to examine the material, political, economic, social, military, and intelligence qualities comprising national power and how each of these aspects of power is dependent on cyber. The argument in support of a power matrix unique to cyberspace is made by building on previous works on power to develop a dynamic and highly evolved understanding of national cyber power. The development of a conceptual understanding of cyber power then allows for operationalization and testing of power within both rational and cognitive frameworks. The issues associated with anonymity, attribution, and asymmetry weigh heavily on the development of power in cyberspace and influence the scalability and relative value for state use.

Following the initial analysis of power, the focus of the chapter becomes developing an index variable representative of the components of cyber power. Broadly a theory of cyber power is comprised of three categories: theoretical capabilities, demonstrated capabilities, and national digital dependence. The aggregate measure of these categories provides a power score, which can be input into the utility theory of cyber conflict developed in the third section.

Power is an ambiguous concept. Power in the traditional sense is imagined as a brute force strength that overwhelms a potential adversary. Or as Jeffrey Hart explains, the definition of power contains the common threads of "control, influence, and legal authority."[1] In politics and international relations in particular, there is one primary type of power, the ability to get one's way. This can be lin-

guistically construed as ability for a person to influence others. Simply put, a weak person is forced, whereas a powerful person forces.

Max Weber wrote of power that it is "the probability that an actor in a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests."[2] The ability to carry out one's own will can be derived from the psychological context, or it can be derived from physical brute force. Hence both psychologically and physically an atomic bomb is more "powerful" than a knife. Here cyber power is dissected and parsed out as a new form of power that straddles psychological and brute force (physical) conceptualizations. Understanding what cyber power is provides insight into how states might decide to wield it, and serves to ground any decision to use cyber weapon systems (CWS) in reality rather than fiction.

Conventional studies on power within rational choice modeling of war have depended largely on physical brute force definitions of power. These brute force definitions include military and domestic production capabilities. The general assumption of power is Hobbesian, referring to a state of nature without a leviathan (governing authority) to enforce laws. A large brute army, with sufficient domestic capacity, can overwhelm a smaller one. As Thucydides wrote in the Melian dialogues: "Right, as the world goes, is only in question between equals in power, while the strong do what they can and the weak suffer what they must."[3]

Concepts of power in international relations have evolved somewhat over the last thirty years led largely by Joseph Nye, who has made it his quest to define more accurately the concepts of power for the modern world. If the concepts of power as they have been traditionally used were wholly accurate in conceptualizing conflict, then organizational advances in military structure would not have greatly affected the battlefields of Europe during the Napoleonic era or during the two world wars.[4] However, as Nye notes, the concept of power is highly complex and breaks down into two broad classifications of soft and hard power.[5] Although the focus here is on hard power, or pushing an adversary to do as you wish, the concepts are deeply intertwined and in many cases indistinguishable.

The arguments on power given here are by no means the first to take up the definitional aspects of power in cyber, and there is no need to redefine cyber power in a wholly novel way. As such this book leans heavily on the terminology developed by Kramer, Starr, and Wentz when they define cyber power as "the ability to use cyberspace to strategic advantage to influence events in other operational environments and across the instruments of power."[6] This definition facilitates what United States Cyber Command refers to as an "intended cyber effect."[7] Although the definition of power is straightforward, the ability to apply the concept in social scientific analysis is lacking. What is required is a way to

operationalize cyber power so that it can facilitate a mathematically based rational choice model.

Operationalization of concepts in cyber is difficult because cyber power transcends many aspects of other domains. This makes measuring the cyber power of a state difficult. The next two sections parse out a workable definition for cyber power in the context of hard applications of power, or what Nye describes as "push" applications of power, rather than "pull." First, what are the constitutive aspects of cyber power that can forcibly influence an opponent? This is composed of several categories of variables: military units for cyber purposes, national ICT human and economic capabilities, legal and regulatory frameworks, technological infrastructure, industry application, and demonstrable threat spectrum capabilities. Second, what are the inherent vulnerabilities of cyber power? Lastly, how do these variables interact to create a measure of cyber power applicable to understanding decisions in international relations?

DEFINING THE COMPONENTS OF DIGITAL HARD POWER

Joseph Nye writes: "Cyber power behavior rests upon a set of resources that relate to the creation, control, and communication of electronic and computer based information—infrastructure, networks, software, human skills."[8] This indicates that cyber power, as an influencing force, is composed of tangible components. As in conventional warfare there are physical attributes associated with the domain of conflict. Infrastructure, networks, and software represent the equivalent of modern combat systems, guns, and bombs. Likewise, as in conventional domains of conflict, human skills and the humans themselves are important attributes. A trained army is more effective than an untrained one.

The variables composing the indexed variable of power within this book are largely derived from Charles Billo and Welton Chang's study, "Cyber Warfare," published by the Institute for Security Technology Studies at Dartmouth College, and the Economist Intelligence Unit's (EIU) "Cyber Power Index," developed with funding from Booz Allen Hamilton.[9] The Dartmouth study contains a highly detailed list of variables in its analysis of the motivation and capabilities of states to engage in cyber warfare. Many of the variables are aggregated in the present work. Specifically aggregated are those capability variables that measure similar attributes. In addition to the variables defined by the Dartmouth study are those defined in the Economist Intelligence Unit's dataset on cyber power. The Cyber Power index by the EIU includes four categories of variables, each of which is included in the overall measure of cyber power. The measures used by the EIU are legal and regulatory framework, economic and social context, technology infrastructure, and industry application.[10] The benefit of incorpo-

rating the EIU's variables into the overall index of national power is an added dynamism to the theoretical conceptualization of cyber power.

The Cyber Power index by the EIU included power scores on only nineteen different nations. This spatial limitation was corrected in two ways. First, data were collected on five additional countries, including Israel, Syria, Estonia, Georgia, and Iran. Data from these countries are from the most recently available year. Second, several of the subcategory variables included in the EIU's data were unavailable for smaller countries. It was deemed these variables were of limited importance. To make up for their absence, the weighting of the power scores was readjusted. All of the weights and the variables included, as well as their sources, are listed in the appendixes.

Below, the components of the theoretical conceptualization of cyber power are explained with their hypothesized effects on cyber power. However, before diving into each of the variables, it is necessary to understand how they are combined to create a single measure of power to be used within a rational decision-making model of cyber.

To create a single robust measure of cyber power, the next step in the process is to develop an index variable of power. This index variable is similar to the Composite Index of National Capabilities (CINC) score. J. David Singer and colleagues, the creators of CINC scores, incorporate variables of conventional power ranging from total population to military personnel within a country, create an additive model, and then divide the summation of the power scores by the number of variables.[11] Each of the variables included in their indexed variable is a country to world ratio, used to represent the finite number of resources presently available to engage in conflict. Equations 4.1 and 4.2 are a representation of this method of indexing to create CINC scores.

Indexing Equations for CINC Scores[12]

$$4.1 \quad Ratio\ of\ Variable\ X_1 = \frac{Country}{World}$$

$$4.2 \quad CINC\ Score = \frac{X_1 + X_2 + X_3 + X_4 + X_5 + X_6}{6}$$

Although Singer and colleagues use a ratio of country to world to express a relationship of power within a finite resource system, this conceptualization is not applicable within the cyber domain. Because the resources and capabilities of the cyber domain expand and are not finite, even in a short temporal range, a ratio for the individual measures in the context of global capabilities in most instances would be meaningless. Unlike conventional capabilities within a physical domain, the cyber domain is virtual and man-made, and its theoretical limits are

unconstrained. Therefore, to create a meaningful measure for power each of the variables is coded using available open source data and placed on a scale of 1 to 10. Variables adapted from the EIU are divided by 10 to give a number between 1 and 10. The variables are then measured relative to other countries to provide a rank ordering of nations in cyberspace. The higher a score, the more capabilities a state has within that aspect of the indexed variable relative to other states.

The components of the indexed variable are as follows: approximate size of information (cyber) warfare units, legal and regulatory framework, economic and social context, technological infrastructure, industrial application, national military budget, and demonstrated cyber capabilities. Lastly, these components are scaled against national digital vulnerability. Each of these variables in some way influences the cyber power of a state.

The first theoretical variable, information (cyber) warfare unit size, is a conventional measure of military strength within any domain. It is important to define the size of cyber units because, just as conventional theorists define the size of standing armies as a measure of power, cyber warfare units represent the number of individuals a state can task on a particular problem.[13] It should be noted that the exact constitution of U.S. Cyber United is classified, as are many other nations' cyber units. Although the exact size and makeup of the units is classified, the approximate relative size of these is important for both offensive and defensive operations. Larger units are capable of writing more code, analyzing and monitoring more systems at the same time than smaller units. Despite the possibility of diminishing returns to scale, diminishing returns are system dependent and therefore not able to be adequately accounted for across nations, time, and space. It is therefore assumed that the more individuals a state places in its cyber units, the more powerful it will be within the cyber domain. Cyber unit size is included because it is hypothesized that cyber power is significantly influenced manpower for operational taskings both offensive and defensive. These data are obtained through open source reports and are not an exact measure of unit size; rather, the data estimate size relative to the state system. As such, a score of 10 for cyber unit size would indicate that a nation has very large dedicated cyber units, whereas a score of 1 would indicate very small cyber units, and a score of 0 would indicate no cyber units.

Similar to conventional warfare, in cyber it also matters how many "boots" are on the ground. Coding, like any great building project, requires manpower. It is hypothesized that as manpower devoted to cyber units increases, so too does the cyber power of a state. The manpower argument works up to the point of diminishing returns. Each type of project within the cyber domain has a different point of diminishing returns, so for simplification it is assumed at present an unlimited movement toward efficiency in much the same way conventional theorists assumed that large numbers would win the day on the traditional battle-

field. While an unlimited movement toward efficiency might seem to be a bold assumption, it is important to remember that a networked environment such as the United States Department of Defense comprises millions of computing devices and thousands of networks, making each addition to a force for offense and defense relatively small in comparison to the overall attack surface.

Boots in raw terms of cyber unit size are not sufficient to account for the quality of those boots. It is therefore necessary to divine a measure adequate not only to measure the military offensive and defensive unit size of states within the cyber domain but also to determine their possible quality. To determine the quality of the potential cyber warfare units here the indexed economic and social context variable developed by the EIU is used. This variable accounts for a range of qualities including educational levels, technical skills, trade, and innovation environment.[14] Higher scores would indicate a more powerful nation within the cyber domain.

An increase in power is hypothesized as an effect of stronger economic and social levels because the more educated, more technical, and more innovative individuals are within a state, the more capable they are likely to be in writing code and developing new hardware and software platforms. Although holding a gun and pulling a trigger are skills that can be reasonably adapted to most soldiers, the writing of code and the maintenance of information communications infrastructure require years of training. Based on off-the-record conversations with individuals involved in training U.S. personnel entering into the coding field, the fail-out rate for potential cyber warriors is far higher that one might think. This makes it difficult to find and retain qualified persons willing to spend time in service to their nation.

The power of a state and its ability to be successful in the cyber domain are heavily dependent on a wide variety of subcharacteristics within an economic and social context. These aspects of cyber power indexed into a single variable represent a human and market capital environment that facilitates offensive and defensive cyber operations. A full breakdown of the components of the economic and social variable as well as all EIU variables can be found in Appendix B.[15]

The economic and social context of cyber power interacts with the next two variables, technological infrastructure and industrial application. The EIU indexes these two variables, each of which comprises multiple sub-aspects.[16] Infrastructure and industrial application are expressions of the robustness of a country's cyber domain. Contained within this variable as defined by the EIU are measures of ICT networks, ICT access, ICT spending as a percentage of GDP, the use of smart grids, digital health, e-commerce, intelligent transportation, and e-government. These measures are reflections of what a nation is doing with the technology it has. Nations at the forefront of leveraging technology infrastructure are often less vulnerable to conventional exploits and lead the world in

innovation and application of that innovation into their critical infrastructure. It is hypothesized that as infrastructure increases in size and robustness, it paradoxically becomes increasingly stable as redundancies make up for potential weaknesses of single choke-point vulnerabilities. More than simply increasing the capabilities of states, these measures pull in tangible qualities that affect the relative cyber power of states.

The technological infrastructure and industrial application ICT of a nation represent the hard-core present environment in which the economic and social context flourishes. The technological infrastructure and industrial application of technology influence each other and can in some respects become mutually reinforcing, creating a technological development pathway. When the economic and social contexts and the technological infrastructure of a state are developed, there are increasing industrial applications for technology. As infrastructure improves, it becomes possible to conduct increasingly complicated industrial activities within the cyber domain including the automated control of traffic systems, subways, and utilities. Although these three variables are measured independently of each other, they are weighted into the index variable for cyber power and combine to provide an important and unique attribute of state cyber power.

Military units, human resources in an economic and social context, the infrastructure, and industrial application of ICT are only useful in the context of their legal and regulatory frameworks. As with conventional conflict, it is important to understand how both sides view potential actions and in what ways they will respond. Legal and regulatory frameworks, as defined by the Economist Intelligence Unit, are composed of government commitment to cyber development through a national cyber plan and public/private partnerships; a cyber protection policy composed of cyber enforcement authority, cyber security laws, cyber crime response, international cyber security commitments, and a cyber security plan; cyber censorship; political efficacy; and intellectual property protection.[17] These legal and regulatory variables all combine to contextualize the organizational and operational aspects of a state's capability within a domain.

A state with a poor legal and regulatory framework in place as indicated by inadequate or poorly defined laws, policies, strategies, and plans will be at a disadvantage over more prepared rivals. Nowhere has this been illustrated better than during the working simulation conducted by the Bipartisan Policy Center's experimental war game, Cyber ShockWave, conducted in 2010.[18] This exercise demonstrated the resultant chaos of a government with few legal and policy frameworks in place for responding to a large-scale attack against the homeland emanating from cyber. Of particular importance during this simulation was the amount of time spent attempting to determine who had the legal authority to respond and what that legal authority constituted.

As recently as February 2013 the Government Accountability Office (GAO) released a report on national strategy, roles, and responsibilities and found that many of the major problems faced with regard to cyber security for the United States have less to do with capabilities and more to do with responsibilities.[19] The report clarifies the need for clear jurisdictional authority currently absent, should a complex cyber attack include civilian, military, and government assets. It is therefore hypothesized that as the legal and regulatory frameworks of a state increase, this has a positive significant effect on a state's cyber power.

This variable is an index variable of legal and regulatory frameworks within nations and is derived from the EIU dataset.[20] The more detailed a framework, the more likely it is a state will not experience the same problems experienced during the Cyber ShockWave war game or highlighted by the GAO. States with more highly defined legal and regulatory structures are better able to assign responsibility to various government and private sector actors to facilitate offensive and defensive actions within cyber. Included within this variable are public/private partnerships. States with low levels of industry or academic collaborations are less likely to have robust dynamic defensive and offensive capacities. The Dartmouth report on cyber capabilities states explicitly that collaborations of states with academic and private entities are an important aspect of cyber power.[21] Understanding who is responsible for what in the cyber domain and defining what constitutes attacks or offensive cyber operations are vital to establishing power within the domain.

Lastly, an overall measure of relative potential military capability is included. This measure is included here as the relative country-to-world military budget. This inclusion is hypothesized to increase the power of a state within the cyber domain as it does in conventional forms of conflict. The larger a state's relative military budget, the more funds it is able to allocate to offensive and defensive cyber operations relative to potential opponents. In many ways this variable distorts overall power scores of states. However, a state that has a larger military budget can conceivably allocate these financial resources toward cyber-related endeavors. Although the relationship between the aggregate military budget of a state and its allocation of funds toward cyber is not direct, the case could be made that the ability to redistribute funds, should the need arise, exists within the military apparatus.

The above measures are each rooted in tangible numbers, yet their effect on the ability of a state to influence or impose its will on other states is less certain. Years of evidence and a host of academic studies indicate a significant correlation between material capabilities available for a conventional war and the increased power of a state, but the same is not necessarily true in the cyber context. Therefore these variables—human, material, legal, economic, infrastructure, industrial, and budgetary—are best regarded as theoretical aspects

of cyber power. Based on theory each of these variables proportionately affects the resultant theoretical scope of power of states in a different way. Building on previous studies and on available data, this book assumes each of these variables affects the resultant power of a state differently. The proportion of their effect is represented in data tables in the appendixes.

Each of the above variables combines to form the theoretical aspects of cyber power of a state. Much as it is possible to look at the statistics of baseball players and determine what the ideal team would be based on a collection of numbers and information, the variables in the above sections all combine to create the theoretical quality of a nation-state within the cyber domain. This is not sufficient for adequately defining power relationships. Two additional features must be added that extend the construction of power beyond a purely theoretical conceptualization. These variables are demonstrated capabilities and national digital vulnerabilities.

The historical context of cyber within a state adds to the construction of an accurate power score by illustrating what a state is actually capable of. Although a state might have large budgets, training programs, collaborations with universities, and industries, each of these attributes of the indexed variable remains largely theoretical until that state demonstrates a threshold level of capabilities in the real world. Just buying and reading books on medicine does not make a student a medical doctor. To become a doctor a student must train with patients and demonstrate his or her abilities. In this context it is important to understand whether a state has conducted or defended against a cyber attack and what the scale and complexity of the attack was.

This type of historical variable is imperfect, but it provides a comparative way of understanding a state's demonstrated cyber capabilities. By adding in actual demonstrated capabilities of states the indexed variable adds actual technical capabilities rather than assuming the construction of a measure of power in cyberspace. For example, the Russian Federation's cyber attacks against Georgia in 2008 would be illustrative of an operational and organizational complexity unique in many respects to the cyber domain. Likewise the Israeli cyber attacks against Syrian air defense systems also illustrate a level of capabilities that differentiates it from other state actors. In this instance it is possible to use a history of actual capabilities to inform a model largely predicated on theoretical capabilities. This variable is separated from the others and constitutes its own multiplicative aspect of the indexed variable. Fortunately there are no states that haven't, to some extent, been tested in the cyber domain. A historical realistic perspective of cyber capabilities is referred to here as demonstrated threat spectrum capabilities. It is separate from the other variables specifically because it is not theoretical in nature. The historical or demonstrated capabilities measure is derived from contextual analysis of cases written up by the United Nations

Institute for Disarmament Research, the Security and Defense Agenda report on cyber security, the Center for Strategic and International Studies and the Dartmouth Report on Cyber Warfare, and Robert Carr's book on cyber warfare.[22]

The data were coded on a scale of capability and complexity ranging from 1 to 8. The scale ranges from cyber propaganda to compromising of hardware systems. The scores were then standardized against one another to fall on a scale of 1 to 10, where 10 represents extensive threat spectrum capabilities and 1 represents minimal capabilities. This score then interacts with the theoretical dimensions of power to provide a numerator of cyber power without taking into consideration national digital vulnerabilities.

The above variables form the top portion of the equation in the indexed variable illustrated in equation 4.3. Each represents a fundamental aspect of cyber power without specifically focusing on what types of systems and computers a particular country uses in its networks and infrastructure. To delve down into infrastructure composition would be extremely difficult and illustrate only moments in time rather than examining the true power of a state within the domain. Although each of these variables creates a model similar to the one illustrated in equation 4.2, it is impossible to conceptualize the cyber domain without adding one more unique attribute that scales power to accurately reflect the real world. Equation 4.3 is a representation for how the indexed variable and its components should be conceptualized within the cyber domain.

Table 4.1 shows the variable names with their corresponding variable codes. The first six variables all proportionately influence cyber power differently. For instance, although it is important to have military units assigned to conduct cyber operations, those units are ineffective without the legal and regulatory framework to organize and control them and the economic and social context providing trained personnel. The theoretical aspects of cyber power are combined to result in a meaningful measure of theoretical cyber power. This measure is then multiplied by the demonstrated capabilities of a state within cyber offense or defense. In this way, we are able to gain a holistic picture of what constitutes cyber power. A complete breakdown of the proportional values for each of the variables is included in Appendixes A through C.

Indexing Equation for Cyber Power

$$4.3 \quad Cyber\ \ Power = \frac{(MUD + LF + ESC + TI + IA + MBA)\ TSC}{NDV}$$

Equation 4.3 represents the construction of cyber power. The present section focuses solely on developing the top portion of the equation. The next section

TABLE 4.1 Components of Power

Variable Name	Proportional Influence	Variable Code
Military Unit Designation	15%	MUD
Legal and Regulatory Frameworks	25%	LRF
Economic and Social Context	25%	ESC
Technological Infrastructure	15%	TI
Industrial Application	10%	IA
Military Budget Allocation	10%	MBA
Threat Spectrum Capabilities		TSC
National Digital Vulnerability		NDV

focuses solely on the concept of national digital vulnerabilities as a way to realistically scale power to reflect the actual operating environment.

CYBER AND ITS VULNERABILITIES

Cyberspace is a porous domain. Whereas in land warfare it is theoretically possible to lay out a line of tanks to form a semi-impenetrable wall, in cyberspace even the strongest firewall has weaknesses. Cyberspace is dominated by billions of systems, millions of security devices, and petaflops of data. Although certain countries are likely to have specific vulnerabilities within their cyber infrastructures, no two countries are likely to be the same. Such a situation would lead to a multitude of models, all with different measures for vulnerabilities. Chapter 7 illustrates that it is possible when focusing on a single target to use intelligence to more accurately hone the vulnerability measure. However, when creating a model attempting to explain cyber power across all actors, it is not possible to delve down into the details.

Cyber vulnerabilities can range from poorly configured systems, old software and hardware, bugs, viruses, Trojans, worms, zero-day exploits, and open ports to insider threats posed by employees with malicious intent or unknowing recklessness. The variations in vulnerabilities are as numerous as the number of systems and the people using them. A case from 2000 illustrates the seriousness of even low-level vulnerabilities.

Vitek Boden worked for Hunter Watertech, an Australian firm responsible for installing the control systems for a county sewage facility in Australia. Upon completion of the contract Boden applied to work for the same county. When his application for employment was denied, he decided to take revenge by driving around to all the various control mechanisms he had helped to install, and via radio link he caused them to release raw sewage into public parks and waterways. The result was an environmental disaster.[23] The case illustrates that vulner-

abilities can arise just about anywhere. There was no system in place to protect against a disgruntled former employee, and the result was a cyber attack.

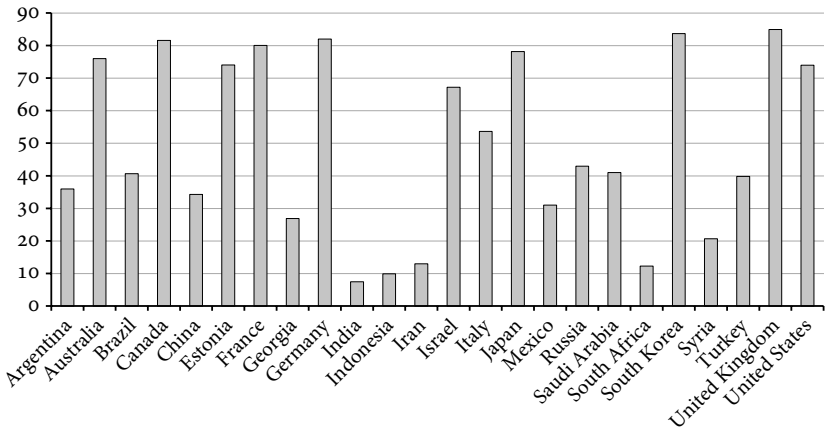
Cases such as Vitek Boden's in Australia are not unique and occur on a regular basis, according to the Secret Service.[24] But this is only one category of vulnerability. Most scholars agree vulnerabilities to the cyber environment are present in almost unlimited forms. This pervasive fear is highlighted by a Government Accountability Office report from 2008 specifically focused on indicating a large number of vulnerabilities present within the national critical infrastructure.[25]

With a near infinite variation in the number of vulnerabilities, what is the best way to operationalize the concept of vulnerability into a measure applicable for conditioning cyber power, and why is this necessary? Vulnerability is vital to understanding power. In 1990 Saddam Hussein had an enormous military with nearly half a million active-duty military personnel. If power were to rely on numbers alone, the first Gulf War should not have been won as quickly as it was. The relative power based on aggregate numbers was not such that it should have facilitated a speedy American victory. However, the Iraqi military had strategic vulnerabilities and command and control vulnerabilities that, when exploited, made it difficult for Iraqi commanders to communicate with deployed divisions. This indicates that power is not a pure numbers game even in conventional conflict; in the cyber world it is even less so.

A nation such as North Korea can develop an offensive cyber unit and ignore the need for a defensive cyber unit because it has little to no reliance on cyber technologies in its homeland. Its economy is not cyber dependent, and its electric grids are not connected to smart grids. The exploitation of North Korean cyber vulnerabilities would have limited substantive national effect. The same was not true of the attacks against Estonia in 2007. The nation of Estonia, sometimes referred to as "E-Stonia," was highly digitally connected. When Russian-condoned "hactivists" used DDoS attacks to assault its media, banks, and government systems connected to cyber, it brought the country to a temporary standstill.[26]

A small state wielding cyber weapons might have a greater degree of relative power than a large state as it has significant theoretical and demonstrated capabilities but few vulnerabilities. The best example to explain this differentiation in relative power would be two equally skilled soccer players or perhaps even a professional goalie and a high school goalie, each defending against a penalty kick from the famous Pelé. The goal the professional goalie is defending is the size of a city block approximately four hundred meters long. The size of the goal the high school goalie is defending is equivalent to that of a hockey goal. Irrespective of how talented the professional goalie is, he is unable to reasonably secure his goal despite his better skills and qualifications because the attack surface

FIGURE 4.1 Percentage of Individuals Using the Internet within Countries in the Sample (2011)



he has to defend is so large. Pelé has many ways he can kick a goal against the professional goalie. Yet against the amateur he must rely on other skills such as anonymity, deception, and other traits rather than sheer physical power to kick the ball if he hopes to score a goal.

What these examples illustrate is that while a state might have a large cyber offensive capability, it might have no defensive needs at all. And while a state might have little to no offensive capabilities, it might have a great defensive need. This poses the question of how to measure this complex relationship between those aspects that enhance the power of a state in the cyber domain and those that increase its vulnerability?

Because it is difficult to isolate specific vulnerabilities of a state and because national security within cyber blurs the civilian/military boundary, this model incorporates an aggregate measure of national digital dependence. The logic behind this measure is simple. The more digitally dependent a society is, the more vulnerabilities it is likely to have. To measure national digital dependence this book relies on the International Telecom Union's (ITU) data on percentage of individuals within a country using the Internet. Figure 4.1 is a graphical representation of the ITU data.[27] The darker the country, the higher the percentage of Internet use and therefore the greater the systemic vulnerability of the nation to threats emanating from cyberspace.

These data are collected by the ITU from national statistical offices and combined to provide the best overall collection of meaningful information on potential cyber vulnerabilities. This variable is measured in the same way as the other variables on scale of 1 to 10 according to percentage of individu-

als within a country using the Internet. It is best thought of as expressing the higher likelihood of vulnerabilities within a nation. It is an imperfect variable as it is unable to account for problems associated with the speed of connection or the frequency of use. It also fails to account for system construction and age or vulnerability of systems. Despite these failings, this is at present the most robust variable on the aggregate measure of vulnerability for nations within cyberspace.

CONCEPTUALIZING CYBER POWER

This chapter examines the concept of power and builds an argument for a measure of power unique to the cyber domain. This measure incorporates theoretical and actual aspects of capability and capacity. The construction of power then moves further than simply capability development and indicates that power in the cyber domain is heavily conditioned on the vulnerabilities of a state. Whereas in conventional conflict, vulnerabilities are primarily measured in the capability and capacity of a state to wage war, in cyber if a state has few vulnerabilities, it also has few targets an adversary can attack or retaliate against.

Equation 4.4 is a representation of cyber power in the simplest possible terms and can be expressed in words with aggregated variables as the theoretical cyber force (F) multiplied by its demonstrated threat spectrum capabilities (T) over its national digital dependence vulnerabilities (D). It represents the absolute power of any one state within the cyber domain. Such a measure can be developed in excruciating detail through the use of intelligence, as is examined in chapter 7, or it can be examined through broader brush strokes as done here.

Equation for Cyber Power

$$4.4 \quad Cyber\ Power = \frac{F\ T}{D}$$

It is important to note that cyber power can be operationalized in such a way as to convey meaning within the cyber domain. This operationalized measure then can be used in facilitating a decision-making model for action within the cyber domain. As should be apparent, the domain is unique from conventional domains and must take into consideration those attributes that best account for a new and evolving form of power.

Based on the variables and their relationships to one another, table 4.2 provides a ranking of the cyber power of each of the states within this work. The table includes two power scores for each country; however, they are ranked

TABLE 4.2 Power Scores by Country (2011)

	Country	Power Score	Weighted Power Score
1	Germany	3.17	9.41
2	Japan	2.03	9.36
3	UK	3.81	9.35
4	South Korea	3.01	9.17
5	Canada	3.24	9.02
6	France	3.20	8.89
7	Australia	3.79	8.36
8	Estonia	2.27	8.27
9	USA	10.86	7.44
10	Israel	9.02	7.27
11	Italy	2.80	5.72
12	Turkey	2.13	4.82
13	Brazil	2.93	4.58
14	Russia	5.56	4.57
15	Saudi Arabia	1.72	4.49
16	Argentina	1.33	4.29
17	Mexico	3.41	3.63
18	China	6.47	3.58
19	Georgia	3.20	3.03
20	Syria	0.98	2.39
21	South Africa	6.12	1.57
22	Iran	7.38	1.33
23	Indonesia	4.87	1.33
24	India	23.24	0.81

based on the weighted model. The unweighted power score assumes an equal weight for all variables and is considered to be of lower accuracy. While the resultant rank order of the weighted power score seems to counter the notion of the United States being the most powerful nation in terms of cyber power, it is important to remember that power score is only one aspect of the probability for success. The next chapter adds to the concept of the probability of success in the cyber domain and examines anonymity's influence on cyber decision-making. Unlike in conventional conflict a raw estimation of power is only one part of the whole decision to engage in cyber conflict.

The above analysis looks beyond the broad definition of cyber power provided by Kramer, Starr, and Wentz and focuses on the push aspects of cyber in the same way Bruce Bueno de Mesquita incorporated CINC scores into his concept of power in his expected utility theory of international conflict.[28] Cyber power is the ability of a state to create, manipulate, modify, degrade, or deny the use of information communication technologies to a target(s), while simultaneously minimizing any and all potential threats against itself. Creating, manipulating, modifying, degrading, or denying the use of ICT allows a state to impose

its will on another. A state with high offensive capabilities and low defensive vulnerabilities within the cyber domain will be considered powerful. Power in this context indicates that a powerful state will have an increased ability to exert its will within the domain and accept the resultant consequences of its actions. A state with greater cyber power will have a relative advantage within the cyber domain over states with lower levels of cyber power. This will be an increasingly important concept as we move forward in developing a rational model for how a state decides when to attack within the cyber domain.

CHAPTER 5

Anonymity and Attribution in Cyberspace

> There is a powerful tension in our relationship to technology. We are excited by egalitarianism and anonymity, but we constantly fight for our identity.
>
> David Owens, "Anonymous 'Takes Down' CIA Website"

> We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.
>
> Quoted in Scott S., "We Are Anonymous"

ANONYMITY AND, BY EXTENSION, attribution are two fundamental aspects of the cyber domain. When a state decides to attack another state, it is not concerned solely with its relative power to its adversary. An attacking state is concerned with the power of its adversary and its ability to conduct an attack against an adversary while maintaining anonymity. Anonymity in cyberspace in the initiation and implementation phases of an attack provides the freedom to maneuver. *Webster's* defines anonymity as follows:

1: of unknown authorship or origin
2: not named or identified
3: lacking individuality, distinction, or recognizability[1]

The analysis below focuses on the origin or instigating actor, the target that is not identified, and the recognition that an attack is occurring. Specifically the concept of anonymity is approached from the offensive perspective of a state considering instigating a cyber attack against a potential opponent.

To understand anonymity it is necessary to ask basic questions of international politics. First, why is anonymity important to a cyber attacker? Second, is it possible to conduct a political act and remain anonymous? Third, why is attribution important to a cyber defender? These three questions are answered below followed by a summary of the importance of understanding anonymity and attribution in offensive cyber decision-making.

THE IMPORTANCE OF ANONYMITY

Most of the literature on cyber attacks makes clear that one of the most valuable aspects of the cyber domain is anonymity. Anonymity is a distinctive asset in covert operations, providing political plausible deniability while allowing for the attainment of a strategic or tactical objective. It is difficult to assess the true value of anonymity in cyber. From an offensive perspective the objective is to remain anonymous as long as possible while still achieving an objective. This is likely to lead an attacker to obfuscate his or her operation. As described in earlier chapters, if a target of a potential attack emanating from cyberspace knows where an attack will occur, or who will perpetrate an attack, it is much more likely to be able to defend against that attack.

Anonymity in cyber is multifaceted. The layers of anonymity are constructed by the following characteristics: the inability to identify a perpetrator (state instigator) of an attack, the inability to recognize an attack is occurring, and the inability to isolate the target or objective of an attack. These characteristics build upon the two characteristics of attribution within Susan Brenner's legal framework for understanding cyber attacks.[2] These three characteristics are important for both legal and practical reasons. As *The National Strategy to Secure Cyberspace* accurately notes: "The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult."[3] Beyond simply being unable to identify the perpetrator, as is often the case in cyber attacks, it is difficult to recognize when a cyber attack is even occurring.

Titan Rain, a cyber espionage operation targeting various defense systems, including U.S. Logistics Command, is an example of a cyber attack that stayed beneath the radar.[4] A defender that does not know an attack is occurring is even less likely to know what the target of that attack is. The Titan Rain incident is particularly difficult to access in its entirety because the stolen data were encrypted on the way out, making it technically difficult to know what the purpose of the attack was and exactly which files were taken.[5] The only way to judge the significance of the attack was to measure the volume of the data taken in terabytes.

Anonymity within cyberspace is a valuable tool to both the perpetrators of attacks and the average user alike. Over the last several years I have worked with democracy NGOs around the Middle East and other regions building training platforms for democracy activists. These websites are designed to offer potential democracy activists the maximum amount of anonymity to protect them against government persecution. In this instance anonymity is a tool that safeguards liberties. This same ability to remain anonymous facilitates nefarious groups and nation-states that wish to do harm.

Although this book is primarily concerned with the decision-making processes of state actors, the quote at the beginning of this chapter by the group

Anonymous is illustrative of the power a disparate group of nonstate actors can have in cyberspace. If states are unable to prevent ad hoc organizations such as Anonymous from taking down the websites of major governmental agencies such as the FBI or CIA, then how is it possible to defend against state actors with infinitely more resources?[6]

Various scholars have indicated that one of the fundamental problems associated with the structure of the Internet is that it was never designed to provide tracking and referencing of users.[7] It is prudent to remember that the Internet as we know it was started as a private collaboration tool between universities and U.S. laboratories under the control of the Defense Advanced Research Projects Agency. In fact, at its beginning commerce was prohibited on the Internet. As the value and the volume of connections has increased, the value of anonymity has been both a blessing and a curse. For a state deciding whether to use cyber as a means of attack against another state, one of its primary considerations should and does often rightly center on anonymity.

The value of anonymity is supported by both anecdotal evidence as well as sound political logic. In every major case of state-on-state hostile cyber interaction, ranging from cyber exploitation (CE) to cyber attack (CA), anonymity has been a central feature. The answer as to why anonymity is a central feature of hostile state interactions within cyber is discussed in previous chapters, but it does not hurt to reiterate its central premise and applicability to the decision to instigate offensive cyber operations within cyberspace.

A bullet or bomb launched from a gun or plane has a defined trajectory. It is possible to harden a target against them with either a bulletproof vest or a bunker. But once that trajectory has been established, the target is typically assured of impact barring some counterballistic system. In much the same way it is possible to harden cyber assets against cyber weapons. Network administrators can build firewalls or air gap networks to protect them against incoming bits and bytes. But unlike the bulletproof vest that works against any bullet regardless of type, up to a certain caliber, a firewall only protects against identified threats. And at the time of this writing it is estimated that there are approximately 200 million different types of viruses, Trojans, and worms.

Furthermore, just as a bulletproof vest offers little protection against a howitzer round, a firewall can be overcome by larger inflows of bits and bytes (a DDoS attack). If a larger round is coming toward an individual, that individual will attempt to fortify himself or herself in a bunker and survive. The same is true of a cyber attack. If it is known that a large-scale DDoS attack will be conducted, network administrators can expand or distribute network infrastructure capacity or engage in other mitigation techniques to weather the attack.[8] If the network administrators do not know an attack is coming, then they are likely to be casualties, as has been demonstrated in many instances including the 2010 "Operation

Payback," in which a group of substate actors from the group Anonymous took off-line via DDoS attack multiple websites including MasterCard, PayPal, and Visa.[9] If advance warning on a cyber attack is available, a network administrator can also take systems off-line and remove targets altogether, making an attack ineffective for want of a target, or the administrator can mass defensive resources or prohibit traffic from certain points of origin.

If the objective of an attack is to make small changes in the defenses of another state's systems, then the goal is to hide those changes for as long as possible. Not only is it prudent to hide the attacker's identity, but it is prudent to hide the knowledge of the attack as well. Once an opponent knows it is being attacked, its security personnel begin implementing defensive measures as a response. Defenders can increase the robustness of their firewall(s), increase their network capacity, or, in worst-case scenarios, remove the systems altogether. The same is not true of conventional attacks. Once an attack is ongoing, it typically must be weathered or responded to.

Any probability for success in cyber is dependent largely on a relationship between the objective of an attack and the ability to remain anonymous to the point at which that objective is completed. Furthermore, even if the anonymity of the attack is lost, the anonymity of the attacker can still be preserved. This makes it difficult, if not impossible, for the victim to retaliate with any meaningful accuracy. The three characteristics of anonymity combine to significantly condition the decision-making process of actors in cyber.

Many scholars note anonymity is a strong characteristic of the cyber domain. Robert Axelrod and Rumen Illiev indicate that anonymity serves as a fundamental aspect of cyber attacks and define the ability to use a cyber weapon in terms of the ability of a cyber resource to maintain stealth and persistence.[10] Their argument for the importance of anonymity is based on data presented by Bilge and Dumitras suggesting that on average over the course of a three-year period only 3–5 percent of hundreds of vulnerabilities in different browsers were discovered and that the average duration of a zero-day attack is 312 days.[11] This would indicate that not only is anonymity often present as a component in the decision to attack, but that it is also an attribute of the vulnerabilities and viruses associated with the systems being attacked. Axelrod and Iliev's data on when to use a cyber resource indicate that the persistence of an unknown vulnerability is nearly 100 percent when not used, meaning that the life span of vulnerabilities is quite significant.

Beyond just the long duration of vulnerabilities available for exploit due to their almost inherently anonymous nature and persistence, Cornish et al. argue that anonymity might also make it possible for certain actors to achieve disproportionate amounts of political utility from identical acts conducted in cyberspace.[12] While it is true a small state can create a disproportionate amount

of harm in cyberspace in ways not possible using conventional military tactics, it is unclear if this state derives a higher degree of utility for cyber attacks over other forms of asymmetric conflict. Instead, because political utility is compared to various options within the toolbox of state, the actual utility of cyber attacks does not change, only its relative value to other options within the overall decision set. For instance, in the case of Stuxnet, the United States had at least half a dozen options for dealing with potential Iranian nuclear development. Israel had fewer options. Economic sanctions imposed by the United States would be far more harmful than those imposed by Israelis because the United States controls much larger swaths of the global market. Under this logic, the value of a cyber attack does not change based on the size of a state; it simply alters its position within the decision set, making it appear more valuable and thus appear to have greater utility than other options. Moreover, as discussed, cyber power is dependent on many factors, among which are the theoretical capabilities of cyber power. It is a lack of these capabilities that limits the ability to conduct highly complex attacks capable of achieving significant impact.

Anonymity provides a means by which to achieve political utility and acts as a facilitator for the application of power. Chapter 7 provides a graphical representation of the scale and complexity of attacks in relation to their feasibility. The larger and more complex an attack, the more likely it is to need anonymity over time. One exception would be distributed denial of service attacks conducted by nonstate actors who want public acknowledgment of their attack but have time-limited utility measures resulting from disruption of services. The relationship of complexity and scale with feasibility indicates an inverse relationship. The more difficult an attack, the more likely it is to be significant in either size, complexity, or both. There are only a few select countries with the technical capabilities to conduct a highly complex attack such as Stuxnet or the attack on Syrian air defense systems. There are nearly a hundred countries and large numbers of substate actors capable of conducting the type of attacks used against Estonia in 2007. The disproportionate relationship between the size of a state and anonymity is directly related to the number of potential actors and the ability to remain anonymous. Although the Stuxnet attack has not been publicly claimed, it has been widely reported as emanating from the United States and Israel through official sources within President Obama's administration.[13] Anonymity was a crucial aspect of Stuxnet, and although the attack has not been publicly claimed, particularly in the first few years after its initiation, the range of possible actors based just on factors such as complexity and scale of attack is quite small. If the attack is contextualized in foreign policy and international relations, the range narrows to possibly three and more likely two actors.

Anonymity is a complex measure. The three characteristics of anonymity are extremely difficult to maintain indefinitely. The key is to prolong a combination

of the characteristics long enough to achieve an objective in cyber. Furthermore, if the identity of the attacker remains anonymous, this denies the legal justification for retaliation by the targeted state as well as denying the identification of a proper institutional format for recourse.[14]

POLITICAL ACTION AND ANONYMITY

Is it possible to conduct a political act and remain anonymous? If we follow the logic of Thomas Rid that "history does not know acts of war without eventual attribution," then do cyber attacks constitute political acts?[15] With anonymity being a central feature that influences the success of cyber attacks, does anonymity remove the political aspect of attacks? Rid goes on to say: "aggressors engaging in subversion, espionage or sabotage do act politically; but in sharp contrast to warfare, they are likely to have a permanent or at least temporary interest in avoiding attribution. This is one of the main reasons why political crime, more than acts of war, has thrived in the cyber domain, where non-attribution may be easier to achieve than waterproof attribution."[16]

This book largely steps over the linguistic gap between what constitutes an act of war and what constitutes a crime or other form of action. For the purposes of understanding anonymity the definition is largely based on the perception of the aggrieved party. However, Rid does make it clear, through linguistic nuance, that certain acts within cyber can contain political utility. Virtually all other scholars agree on this point.[17] While the linguistic distinction between war and political crime has caused a degree of animosity within the subfield, this animosity is likely misplaced and represents different linguistic traditions and conceptualizations of the state of modern conflict in regard to historical frameworks.[18]

The focus on the debate over whether anonymous acts that take place constitute different types of conflict is dependent on the framework of definitions a scholar uses. What is evident is that regardless of how cyber attacks are referred to in the conventional typology, they are capable of generating utility, as demonstrated in chapter 3.

THE VALUE OF ANONYMITY

Acts that occur in cyberspace are not necessarily anonymous, yet anonymity is a desired characteristic for the conduct of offensive cyber actions. How then can we operationalize the concept of anonymity within a rational choice decision-making model so it is logical to the decision-maker?

Bruce Bueno de Mesquita's utility theory simply compares the power scores of different states. By using a capability (power) relationship between states he is able to determine the probability of success for the instigator of a potential

conflict. It is this probability of success that greatly affects the decision to engage in an act. In theory it would be possible to use Bueno de Mesquita's model to explain any type of decision to engage in interstate interactions ranging from diplomacy to war. It would be possible to rearrange the probability function of the model to incorporate those characteristics that influence successful diplomatic interactions to derive a model for bargaining. However, Bueno de Mesquita's model is focused on overt conflict. He uses power to assess the probability of success. Yet because he works in a domain of interaction where distance has an effect, his power relationship is scaled by distance.[19] Distance, as examined in previous chapters, does not matter in cyberspace as it does in conventional military encounters because cyber attacks can occur with no diminishing capability due to distance. A virus code in China does not need to be resupplied by a virus code in the United States. What does affect the probability of success is time. However, the probability of success affected by time does not interact with the power of a state, as is often the case in conventional conflict. Instead it influences the overall probability of success.

There are several ways to represent the relationship to time in mathematical models and probability. One of the more standard statistical methods available to test time to an event is to use a hazard or survivability model. This model is not noting the changes in the power relationship over time; rather, it is examining the probability any given type of attack can remain anonymous within the three above combined characteristics long enough to achieve the objective of the attack. More simply, it examines how long until the target knows it is being attacked, knows the target of the attack, and knows who is doing the attacking.

This is important to the development of a decision-making model for the instigation of cyber attacks, as has been mentioned several times. Once a victim recognizes an attack, it can begin taking defensive measures to protect itself. Once it knows the target of the attack, it can harden that target. Once it knows the perpetrator of the attack, it can begin retaliation. The question the decision-maker then asks is what is the probability at a point from time t_i to time t_c or from instigation to completion of the attack that the instigator is able to maintain anonymity. This probability changes over time. At time t_i, the initiation of the attack, the likelihood that anonymity is lost is relatively low. The longer the attack takes to complete, the more likely the attacker is to lose anonymity. This then becomes a fluid measure expressed in moments in time that can be graphed. Because each type of attack is unique, no two hazard models are the same.

The hazard model is composed of those factors essential to maintaining anonymity discussed above. It is important to know the scale (S) of an attack. The larger the attack, the more difficult it is to accomplish. Next it is important to understand the complexity (C) of the attack. The more complex an attack, the

TABLE 5.1 Probability of Maintaining Anonymity by Attack

Propaganda	99%
Web Vandalism	95%
Denial of Service	90%
Distributed Denial of Service	85%
Cyber Exploitation	80%
Equipment Disruption	70%
Critical Infrastructure	60%
Compromised Hardware Systems	50%

more difficult it is to accomplish. These two variables interact as well. A large and complex attack is more difficult than a small, complex attack or a large, simple one. Next, as mentioned above, it is important to contextualize the attack by determining the level of hostility (H) between nations. If state X has only two primary adversaries, it can quickly isolate the instigator of an attack against its interests. By understanding the level of hostility, it is possible to begin narrowing the number of countries in the system. The more potential actors (Q) within a grouping, the more likely a perpetrator is to remain anonymous. The expression of the hazard function is listed below in equation 5.1.

Hazard Function for Anonymity

5.1 $$A = \log h_1(t) = a + C_i\beta + S_i\beta + (C_iS_i)\beta + H_i\beta + Q_i\beta + e$$

Using this function with complete data, it is possible to isolate at any given point in time from the initiation of an attack to the completion of an attack the probability of maintaining anonymity across the three characteristics of anonymity. As is examined in chapter 7, this model can be greatly influenced by the collection of intelligence. Such intelligence would influence all variables within the above hazard function.

Because there is an assumption of anonymity necessary to instigate any attack due to the characteristics of cyber attacks as defined above, the model in this book is not filled in by data. Instead the probability of maintaining anonymity at the point of initial decision to instigate an attack is kept constant at 1. The probability of maintaining anonymity changes over time. Therefore anonymity at time t_0 is always kept at 1. The probability of anonymity at $t_{0\to n}$ is here defined by the type of attack, rather than using the hazard function for which data are not available. Attacks are broken into eight categories, each with a probability of maintaining anonymity over time. The categories and their corresponding probabilities are listed in table 5.1. These probabilities are anecdotal and as-

sumed. Actual probabilities for each attack would depend on the intricacies of the attack, the hostility between nations, and all of the other features included in the hazard function for anonymity.

The above indicates that the more complicated the attack, the more difficult it is to maintain anonymity. Although the numbers are rough, they are meant to illustrate the intersection of all three categories of anonymity. Many groups and organizations can participate in web propaganda, and it is therefore a low-level and common form of attack. Only a few states are currently capable of fully compromising hardware systems; it is therefore more difficult to maintain anonymity during such an attack.

ANONYMITY, ATTRIBUTION, AND DECISIONS

Although many works focus on the term "attribution," here the focus is on anonymity. This has been done for several reasons. First, an anonymous actor is one who avoids attribution. Many legal scholars, including Susan Brenner, tend to focus only on the attribution aspect of cyber. They do this primarily because they are concerned with the defensive capabilities of states. The ability for states to respond to cyber attacks and their perpetrators is an important aspect of cyber defense. But when we consider the offensive strategy of a state, the concern is a combination of achieving the objective and avoiding attribution. For an attack to gain political utility, a state must achieve its stated objective. If a state cannot achieve even the minimum threshold of its objective, an attack remains unattributed if it did not gain any political utility. Anonymity is a fundamental aspect of offensive cyber operations (OCOs). Attribution is a fundamental aspect of cyber defense. The focus of this book is on developing a model that examines how states decide to attack; therefore attribution is largely ignored from a defensive orientation except where it affects the probability of success.

Wheeler and Larson define attribution as "determining the identity or location of an attacker or an attacker's intermediary."[20] Once a targeted country begins the attribution process, it is often after an attack has been completed. It is doubtful that the Israelis cared that the Syrians knew they invaded their airspace to bomb the nuclear facilities. They had already gained the benefit they sought. The Syrians did not respond militarily because they had already lost that which they sought to protect. In cyber it is more important to identify that an attack is occurring, what the target of that attack is, and how to prevent the achievement of an attacker's goal, than to in the moment identify who is actually conducting the attack.

Deterrence does not work the same in cyber as in conventional conflict. Simply identifying the attacker and threatening response is typically not possible. And even when it is possible, it is only feasible with a cross-domain re-

sponse. Such a response would likely escalate a conflict significantly with unforeseen consequences.

The response mechanism to a cyber attack is theoretically confined in the short term to cross-domain actions due to an inability to quickly and efficiently plan meaningful on-the-fly attacks against an adversary. Cyber attacks are tailored to specific systems and require extensive planning and development to be successful. Unless the groundwork was laid out in advance, making it possible to conduct retaliatory in-domain attacks, a state's primary function is to remove the first two characteristics of anonymity by determining that an attack is occurring, and second, what the target of that attack is.

Joel Brenner created a hypothetical scenario in which attribution is attained but matters far less than the recognition that an attack was occurring and a comprehension of the target of that attack.[21] The scenario is one in which the previously laid groundwork for a coordinated attack against U.S. critical infrastructure begins to take down vital U.S. systems coinciding with a foreign policy flap occurring with China. The decision-makers are paralyzed because at first it is not known whether the critical infrastructure malfunctions are due to an attack or normal error. As the malfunctions continue to occur, it becomes apparent the malfunctions are due to an attack and not an error. Although the likely attributable source is China, that is of little importance. The anonymity of the attack and the targets of the attack are more important than pointing fingers. The ability to hide an attack and the target of an attack facilitates it. In Brenner's case, by the time it was recognized as an attack it was too late to do anything, let alone isolate future targets, and the United States didn't have assets in place to retaliate in kind. Brenner notes that a cross-domain response would have been a prelude to all-out war with unforeseen consequences between two nuclear-armed states. The systems affected were such that even the kill switch mechanism once proposed in Congress would not have been of much use.[22]

Moreover, to publicly attribute the system failures within the U.S. critical infrastructure without having a means to stop them also has many negative side effects. Such an attack could compel the defensive party to work in tandem with the attack initiator to maintain their anonymity. Should information on an attack become known, it could severely degrade public confidence in critical infrastructure and cause widespread panic. Furthermore, without being able to identify the various targets of the attack, the defender risks inciting even more damage against its systems. In this particular case Brenner indicates that the Chinese were using a cyber attack to prevent an armed military response while they asserted control over vast swaths of sea. When engaged in defensive cyber operations (DCOs), it is more important to know that an attack is occurring and what the targets of that attack are than it is to attribute the attack to a particular actor. But because the systems we depend on every day for every aspect

of national security and stability are subject to their own problems, it can be difficult to identify when hostile activity is occurring and when a system is malfunctioning due to purely technical issues not resulting from an attack.

SUMMARIZING THE DEBATE

Kenneth Geers accurately sums up the need for attribution when he writes: "The challenge of cyber attack attribution means that decision-makers will likely not have enough information on an adversary's cyber capabilities, intentions, and operations to respond in a timely fashion."[23] Attribution is a defensive necessity. Anonymity is an offensive necessity.

The probability of maintaining the anonymity of an attack and a target is equally important to maintaining the anonymity of the actor involved. The above analysis attempts to focus on the offensive dynamic of the anonymity-attribution debate and outline a solution for assessing the probability for maintaining anonymity at specific points in time during an attack through social scientific and technical methods. The probability for maintaining anonymity influences the probability of success in a cyber attack as much as the relative cyber power of the state engaging in the cyber attack. Adding a measure of anonymity into the decision-making model adds to the robustness of its findings and facilitates a more accurate understanding of when a state will decide to engage in offensive cyber actions.

CHAPTER 6

Cyber and Conventional Operations

The Dynamics of Conflict

THE DECISION TO ENGAGE in conventional conflict has remained largely unchanged for centuries. Over the millennia there have been no fundamental alternatives to conventional kinetic action. This changed with the creation of a virtual domain of interaction and has created a new threat spectrum applicable within both the virtual and the physical. The analysis below examines the decision to engage in cyber attacks as either stand-alone attacks or in combination with conventional attacks. It does so by examining cyber in the context of the strengths and weaknesses highlighted in previous chapters. To achieve utility, a cyber attack can be a stand-alone event or can occur in conjunction with conventional military attacks and act as a force multiplier or force enabler. Cyber power, similar to Giulio Douhet's proposed uses for airpower during World War I,[1] illustrates that new technologies can offer new vectors of attack but do not necessarily achieve, by their ends alone, the objectives of those attacks sufficient to generate political utility.

This chapter is broken into several sections. The first section examines the meaning of conflict and why it is important when examining decisions to accurately frame the context of the decision on a scale of conflict. The second section focuses on the combinatory power and effect of cyber and conventional tactics and hones in on how a decision-making model could be constructed across two different types of capabilities measures, both influencing one another. The third section returns to single-domain focus on offensive cyber operations and examines their place within the scale of conflict and highlights the necessity of specified objectives. The chapter concludes with a summary of the main points.

THE LANGUAGE OF CONFLICT

Previous chapters avoid the linguistic debate pertaining to conflict that this chapter by necessity directly confronts. Although the specific lexicon is danced around in the opening chapters, it is important to differentiate the levels of conflict themselves and the relationship of utility to conflict. Whereas in overt

diplomatic bargaining it is possible to achieve political gains and losses, these gains and losses are easily understood along a scale of gain and loss. There is no realistic expectation of complete subservience of one party to another. Or as Fearon illustrates, there is a bargaining range in which both sides attempt to negotiate for the best possible deal. The same is not true in war.

In war the traditionally conceptualized objective has been total victory or the forced submission of an enemy to one's will. Clausewitz writes: "If we wish to gain total victory, then the destruction of his armed forces is the most appropriate action and the occupation of his territory only a consequence."[2] War in the Clausewitzian sense is an all-or-nothing endeavor; victory in its totality is the objective. Wars are waged to provide unambiguous policy shifts for a political reason. They are not waged for strategic ambiguity. It is therefore easy to define war as a concept that is far in excess of mere diplomacy. The bargaining range of war is designed to force an absolute position on another country. The Clausewitzian conceptualization of war has been largely adequate for wars waged as pitched battles between armies staring each other down on the battlefield. War is imagined as two or more armies banging into one another until one side acquiesces. Unfortunately this largely physical and kinetic concept of war falls within a pre-twentieth-century conceptualization. According to Clausewitz, "As a total phenomenon its dominant tendencies always make war a paradoxical trinity—composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason alone."[3]

Clausewitz's definition of victory and war is robust, but as Jan Angstrom and Isabelle Duyvesteyn indicate in their edited volume, war has largely changed.[4] The bargaining range rarely if ever is simply defined. Victories have largely become ambiguous and limited. The involvement of populations in war has not had the same effect as Clausewitz once imagined. And in truth, declarations of war themselves have largely fallen by the wayside in favor of more ambiguous terms such as "operation" and "action." As Zelizer notes in the context of American movements toward conflict, there has been a significant shift away from formal declarations of war as the concentration of power has focused on the office of the executive.[5] "War" has become a term unused in explaining most forms of modern conflict between states except in the popular vernacular for conflict. Therefore it is necessary to establish the idea of interstate conflict independent of war and within the constraints of defined objectives.

Conflict can be placed along a scale with war defined in Clausewitzian terms as the furthest point along the scale, the point at which violence, hate, and enmity become so strong that the physical, brutish nature of war moves toward a total engagement. War, as the ultimate form of conflict, would be relatively

unambiguous in its eventual outcome and provide an eventual winner(s) and loser(s). However, as modern history illustrates, most conflicts are highly ambiguous and often have no ultimate objective, but rather a series of objectives that shift over time. A scale of conflict can be seen in most modern forms of interstate aggression. The goal of one state is not to permanently dominate another state, but rather to establish an allied state capable of altering its stated policy objectives in accordance with the victorious party. Because war has largely been constrained in its total form, the objective of conflicts below is no longer merely to eliminate the enemy but rather to coerce it.

The Department of Justice lists at least 125 instances of undeclared conflict prior to 2001 by the Office of the President.[6] The large number of conflicts that have gone undeclared far exceeds the five formal declarations of war and the thirteen authorizations for military engagements. The sheer volume of conflict indicates a utility involved on some level; otherwise such conflicts would be irrational and would not have been repeated with such frequency. If conflict can occur without war, and both the formal declaration of war or engagement in military activities is not necessary for conflict to occur, then how is it feasible to reconcile conflict within and across different domains? How can we examine when it is rational and when it is not to engage in conflict?

Bueno de Mesquita and numerous other scholars define war in terms of casualties. The Correlates of War (COW) project fails to define war according to its outcome and rather defines it by its costs.[7] COW largely avoids the term "war" in its internal definitions and instead ambiguously uses the term "militarized interstate disputes."[8] War has become a term determined by break points assigned by scholars in datasets with different datasets defining war at different levels of casualties. This mathematical definition does not equate to the philosophical definitions from Clausewitz or vice versa. Although Erik Gartzke wrote that mathematically war represents the "error term," it is perhaps more accurate to say war is measured in terms of loss.[9] But decision-makers don't think of war in terms of loss of soldiers and land; they think of war in terms of gain and loss ambiguously. If a president sending soldiers off to battle were to dwell on each and every soldier lost or injured, he or she would have surely not made the decision to engage in the battle. Conflict, in all its forms, is largely disembodied and examined in terms of utility. Conflict at the highest decision-making level is economic and rational. Because there are divergent terms defining both war and what constitutes a victory in war, a utility calculus assists in looking purely at what each side hopes to gain by instigating a conflict and helps us to understand what tools are needed to accomplish a given set of objectives.

To understand the dynamics of conflict and the relationship of cyber attacks in the broader field of conflict studies, it is helpful to take a step back and

examine other forms of attacks in the context of a scale of conflict. This book is different from Bueno de Mesquita's work in that it does not subsume all conflict into the same generalized rubric defined generally as war. Instead this book focuses on the decision to engage in cyber conflict. Cyber is a domain of war fighting as defined by the Department of Defense, and cyber weapon systems are a cross-domain tool of warfare. To understand what it means to engage in an offensive we must place it within the context of conflict and war more generally. To do this it is necessary to follow in the footsteps of other technologies and domains preceding it.

World War I saw the rise of airplanes as a strategic tool of the battlefield. Giulio Douhet, an Italian air power theorist, believed that airpower could quickly and effectively end wars through strategic bombing. He was followed by the likes of Billy Mitchell and others continuing to the present who believed airpower to be a tool sufficiently capable of winning wars. Robert Pape notes that in World War II only about 18 percent of American bombs fell within a thousand feet of their intended targets.[10] He further finds that these numbers improved to 70 to 80 percent of munitions falling within ten meters of their intended target by the Persian Gulf War.[11] However, in neither instance was airpower capable of unilaterally winning a war in the context of the objectives stated by the decision-maker. In World War II, it was believed that strategic bombing would cut off the German war machine and demoralize the civilian population. Although it had a significant effect on the former, it did little to the latter. Furthermore the bombing alone was incapable of halting the German army.

Michael Horowitz and Dan Reiter examine the ability of states to use airpower to coerce an opponent in conflict and largely support Pape in his assessments.[12] They find the ability to coerce an opponent is also due to the availability of targets to put at risk through strategic air campaigns. However, all authors indicate that airpower alone is unable to win a war in the Clausewitzian sense. Although it is conceivably possible to use a nuclear bombing campaign to completely obliterate an opponent nation, the result would likely end in a negative utility as at best the land would be uninhabitable, and at worst the attacker could expect a similar retaliation in response, resulting in a net loss.

Deciding to engage in any type of conflict requires an examination of the scale and objectives of the conflict. Total domination of a state generating absolute victory is often not possible or desired. An accurate understanding of what the goals are can facilitate an accurate assessment of what tools are needed to accomplish an objective. Whereas World War II required total societal mobilization for victory, rarely has this type of effort been undertaken. The next section focuses on the use of a combination of tools to achieve defined objectives less than the all-out conduct of total war.

COMBINATORY ATTACKS

In many types of conflict is it necessary to combine tools across domains of interaction to achieve a desired objective. This is referred to as a combinatory attack. As examined in the previous section, it is necessary to establish the objective of an attack to determine what types of tools are necessary. While it is illogical to use certain tools out of context, in other applications the combination of tools can serve to enhance functional capabilities of one or both tools.

If we return to the airpower examples from the previous section, Daryl Press indicates that airpower used in the Gulf War limited the ability of the enemy to successfully reinforce its lines and created gaps in which ground units were able to exploit weaknesses.[13] Press finds that the use of airpower facilitates a coordinated strike in war and increases the likelihood of a Clausewitzian-type victory, but it is unable to produce one independent of other tools. The combinatory approach examined by Press was, however, facilitated by the command and control warfare mechanisms as examined in detail in Alan Campen's edited volume on the first Gulf War.[14] Campen and others note that the first Gulf War was facilitated by multiple tools all working in coordination with one another. Cyber alone would not have been able to achieve the objective of removing Iraqi forces from Kuwait, nor would a strategic bombing campaign. The result was a coordinated effort of cyber, ground, and air units. This led to what Press and others note as the use of C2W generating a functional application of tools resulting in the increased efficiency of the conduct of conflict.

Within the cyber and conventional debate there has been an ongoing feud over the capabilities of cyber to accomplish military objectives. When Thomas Rid writes that cyber war does not and will not exist, he is correct in the Clausewitzian sense. Cyber, just as airpower, is incapable of winning an absolute victory over an opposing force. Therefore cyber war, just as air war, is more a popular term than a functional descriptor of reality. Cyber conflict does exist and does in fact work to achieve objectives both in conjunction with conventional military technologies and independent of them. Just as airpower can greatly enhance the effectiveness of a ground army and enhance the projection of force against an enemy, cyber weapons offer similar capabilities.

Richard Clarke, a former national coordinator for security, infrastructure protection, and counterterrorism, was one of the first to write about the combinatory strategy of the Israelis in their operation to bomb the Syrian nuclear facilities.[15] Whereas the United States has been known to use stealth aircraft to infiltrate and bomb targets in foreign airspace, few other nations possess this technology. Typically in an air attack a state will use radar-jamming devices to prevent surface-to-air missiles (SAMs) from shooting down their planes. This tactic has some obvious drawbacks. Instead of a state entering into another

country's airspace undetected, this method alerts everyone to its presence and essentially works by preventing SAMs from being effective. The Israeli attack on Syria's nuclear facility was unique in that it neither utilized stealth technology nor employed radar jammers. Instead, the Israelis first conducted a cyber attack against the Syrian air defense system. This attack allowed the Israeli planes to enter Syrian airspace undetected without stealth capabilities to bomb their targets and exit the airspace without their planes even showing up on Syrian radar. This is a clear combinatory attack facilitating a conventional tool, airpower, with a cyber tool, to achieve a limited objective to gain utility.

The Syrian example is not the only instance of this type of tactic. In 2008 prior to the instigation of hostilities between Russia and Georgia, Russian hackers began to systematically target Georgian governmental and media outlets. While the attack was not nearly as complicated as the Israeli attack, the effect was to slow or minimize the communication capabilities of the Georgian government with its own people and the rest of the world. This isolationist tactic likely increased the ability of the Russian invasion force to conduct its operations. Conventional tactics along the same lines have included the bombing of communications facilities and power stations to eliminate the enemy's ability to effectively employ C2W over its defense forces. The Russian case is one of the first instances in which the physical structures were left largely undamaged while still achieving largely the same effect.

Christopher Bronk, a former State Department official and cyber researcher at the Baker Institute at Rice University, provides a scary foreshadowing for potential combinatory attacks in an article titled "Blown to Bits." Bronk sets forth a scenario in which China uses a new type of computer virus to effectively hinder the operation of U.S. command and control capabilities. In his story he hits on a large number of areas in which a combined cyber and conventional strategy can assist in the conduct of conflict. The creation of confusion within an enemy's leadership limits an effective response. Similar to a Pearl Harbor strategy like the one the Japanese hoped would effectively cripple the U.S. response to their aggression in the Pacific with a massive strike against the U.S. Pacific fleet in 1941, the attack by the Chinese in Bronk's story cripples the ability of U.S. forces to mount effective response actions against China.

In each of the three above examples cyber is employed in a capacity referred to as a "force multiplier." A 2005 Pentagon report to Congress states: "China's latest Defense White Paper deployed authoritatively a new doctrinal term to describe future wars the PLA [People's Liberation Army] must be prepared to fight: 'local wars under conditions of informationalization.'" This term acknowledges the PLA's emphasis on information technology as a force multiplier and reflects the PLA's understanding of the implications of the revolution in military affairs on the modern battlefield."[16] This assessment is confirmed by further

testimony in 2011 stating, "these capabilities are being developed as weapons which themselves produce strategic effects as well as serving as key force multipliers for conventional 'kinetic' warfare operations."[17] Other reports indicate that China is not alone in its assessment that cyber is a force multiplier. They are joined by nation-states such as the United States and Russia, as well as substate actors including various terrorist organizations.[18]

Cyber can be used to enhance various aspects of conflict across domains of operation. Cyber can be used for information-sharing purposes, it can be used to hinder information sharing, it can be used in psychological operations against foreign armies, it can immobilize targets with digital components, and it can be used as an enhanced recruitment and training tool for warriors around the world. The term "force multiplier" can mean many things; however, in the military context it refers to attributes that make a given type of military force more effective than if such a multiplier were absent.

Although the term "multiplier" would indicate a straightforward mathematical relationship between the conventional force and its multiplier, the relationship is not straightforward. It is not possible to combine the probabilities of the success of a cyber action and the success of a conventional action in order to gain a complete understanding of the probability for success in any type of conflict in all situations. The Russia-Georgia War example highlights a simple example of why such a probability function would be inappropriate. Although Russian forces used the degradation in information communications capabilities of their Georgian counterparts to their advantage, their overwhelming force and military capabilities effectively assured a conventional military victory. This is not to indicate that if this cyber multiplier had not been present that the utility would have been the same. However, the relationship is not direct in this instance.

The Israeli case nuances the multiplier debate. If the cyber attack had been unable to hide the Israeli actions, the attack would have had a significantly lower probability of success. This indicates a direct relationship in the force multiplier of cyber.

"Force multiplier" is a generalized term, as not all conventional attacks require a force multiplier to succeed. Yet often this force multiplier can condition the overall utility calculation. It is important when constructing a combinatory model that involves cyber and conventional tactics in which cyber acts as a force multiplier to take into consideration the effect cyber has on the overall probability of success. Not all types of conflict carry with them the same relationship. Just as in regression modeling it is often necessary to interact variables in different ways, the relationship between a conventional attack and a force multiplier such as cyber needs to be interacted in different ways. Once this relationship is understood in the context of the particular military action, a dynamic decision-making model can be developed.

STAND-ALONE CONFLICT

Cyber can be used as an independent tool for accomplishing military and strategic objectives. The stand-alone quality of cyber is predicated on attacking those targets specifically attached to or impacted by cyber. Whereas airpower is typically limited to the destruction of targets or the maintenance of zones of denial, cyber extends across multiple facets of national security, as illustrated in chapter 2. Using cyber as a stand-alone tool in conflict requires an accurate understanding of its capabilities, as is further examined in chapter 7. This section, however, contends that with specified and realistic objectives cyber can independently accomplish these objectives without assistance from other conventional tools.

Amit Sharma indicates cyber can be used as a strategy of warfare independent of other tools by harnessing its ability to affect what he refers to as the trinity of national security.[19] Sharma defines the components of the trinity of national security as government, military, and people (economic).[20] A cyber attack, he argues, can overwhelm simultaneously different aspects of the trinity and provide what amounts to a Clausewitzian victory. Although he attempts to make a valid point and follows a logical train of thought throughout his argument, his thesis suffers dramatically in its ability to provide any meaningful examples of such an event occurring. This is not to say that it is not possible, but rather that it is unlikely given the current state of technology.

More reasonable estimations of conflict are found in practical applications of current technologies to actionable strategic and tactical objectives. The best example of a stand-alone cyber attack achieving an actionable objective was Stuxnet. Stuxnet specifically targeted a system of an opponent state and damaged its functional capability. This damage slowed the acquisition of a capability deemed to be politically unacceptable by the attacking nations. Stuxnet is an example of a cyber tool achieving, with relative accuracy, a specific objective in cyberspace. Although there have been some reports indicating that Stuxnet's intended effect might have resulted in increased Iranian production or might have been of little overall consequence, in-depth analysis of the International Atomic Energy Agency's own reports and records indicates that the claims of increases in production were the result of declared reporting under nonproliferation protocols.[21] By most accounts the effect was direct and impactful, although limited due to coding errors that eliminated its cover of anonymity.

One of the problems associated with stand-alone attacks dependent on positive intended externalities is that they often make assumptions about the results of an attack not supported by the direct action effect of the attack. As Horowitz and Reiter note, air power is often assumed to be a coercive instrument of military force, yet the coercive nature of the tool is not related directly to its effect.[22] Instead it is an indirect result. Likewise, had the intended objective of the Stux-

net attacks been to cause Iran to give up its nuclear program, Stuxnet would have been largely ineffective.

According to Joel Brenner, malicious coding instructions embedded in pipeline management software stolen by the Soviet Union in the 1980s had the indirect goal to disrupt Soviet oil production capabilities and the effect of creating physical damage to a single pipeline.[23] In this instance the direct goal of creating an explosion facilitated an indirect goal that followed logically from the direct goal. However, much like lining up dominoes, it is important to understand how one domino falling at point A can eventually effect a different domino's collapse at point F. This indicates one of the fundamental flaws in Sharma's argument that cyber can be used as a tool to wage and win a Clausewitzian type of conflict. The more moving parts that are added to a particular chain, the more difficult it becomes to ensure that all the dominoes fall in the correct order and with the proper force.

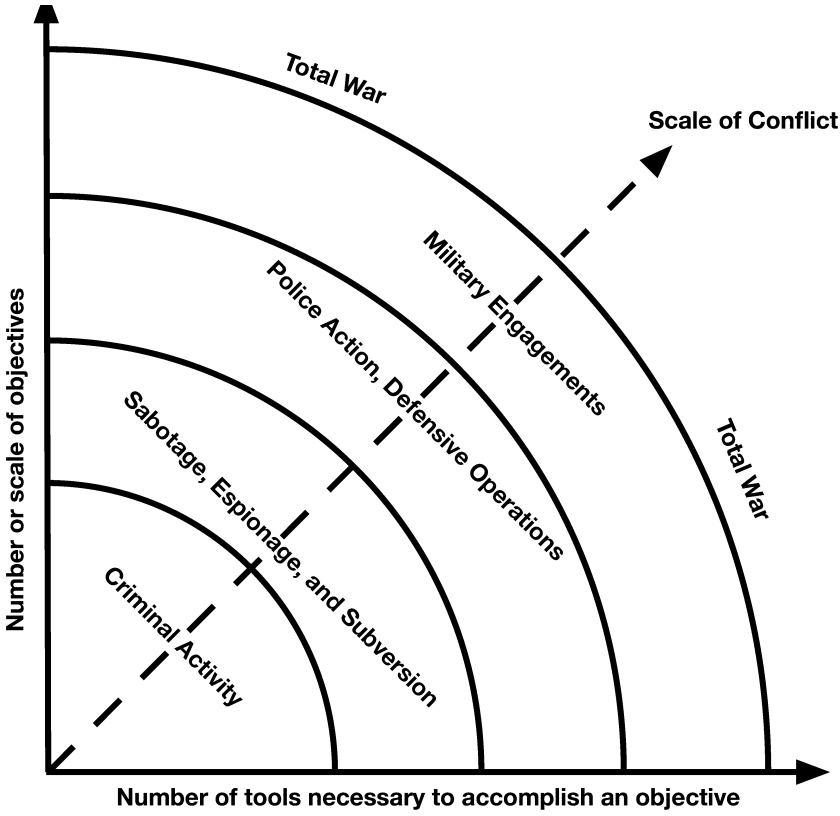
Cyber weapon systems can be a powerful tool that crosses over multiple domains, but it is very difficult to plot the indirect consequences of any given offensive cyber operation beyond its initial objective. As the blitz on London demonstrated during World War II, while the bombing inspired fear, it also hardened resolve, having the exact opposite effect of the intended indirect externality. A cyber attack that disrupts an electric grid might have succeeded in turning out the lights, but it also may have caused car accidents and other hardships on citizens that might result in unintended consequences.

CYBER AND CONVENTIONAL TOOLS: A TALE OF OBJECTIVES

Understanding the decision to attack first requires understanding the objectives of a potential attack. Conflict is a tale of objectives. The larger and more complex an objective, the more tools are required to achieve it. War in the Clausewitzian sense historically requires all available tools. As societies become more and more connected through cyberspace, the need for using cyber tools in conflict increases. However, as the Department of Justice numbers indicate, Clausewitzian wars occur few and far between. What is left is a range of military encounters with a diverse set of objectives spread over multiple points in time. Because no two encounters are identical, it is useful to have a robust "tool bag" of weapons. And while frequently weapons will be used in conjunction with one another, often a limited objective may require only a specific tool. Objectives dictate weapon selection; weapons do not dictate the objective. Understanding the objective of a type of attack defines how the utility calculation should be formulated.

Figure 6.1 illustrates the relationship of conflict, tools, and objectives. Although the figure gives only the roughest of outlines for conceptualizing conflict, it does provide a concise visual overview.

FIGURE 6.1 Objective, Scale, and Tools of Conflict



As figure 6.1 illustrates, there is a relationship between the number or scale of objectives of an attack and the number of tools needed. Similarly, overall scale of conflict increases in size in comparison to the number and scale of objectives and the number of tools employed in a conflict. Although the relationship is not as direct as this figure would indicate, there is a general relationship between what is being requested and the eventual size of a conflict. With this figure in mind, it is evident that a tool such as cyber is unlikely to be the sole tool engaged in a large-scale conflict with a large number of objectives. Despite the way in which cyber crosses domains, it is unlikely to be able to take the place of an occupying army or a bomb dropped from a plane.

Although the analysis here focuses on the relationship between stand-alone and combinatory types of attacks, this book primarily focuses on demonstrating how stand-alone attacks can be examined as generating utility. This is a necessary step, with an eventual goal of being a thorough understanding of how

the utility of any type of attack, combinatory or stand-alone, can be calculated. Bueno de Mesquita sufficiently explains how utility can be examined in the context of conventional conflicts, but as has been explained, the virtual and physical nature of cyber conflicts renders his model inadequate for cyber attacks.

What should be taken away from this is that cyber is a tool capable of working with other tools used in conflict, as well as independently from them. Terms such as "ground war," "air war," "cyber war," and "space war" are vernacular terms denoting the domain of operations for a particular type of conflict; they do not denote the conflict itself. It is far more accurate to conceptualize these aspects as "cyber battle," "ground battle," and "air battle." Although Bueno de Mesquita and others refer to the utility of war, these scholars are subsuming many variables into a single mathematical variable. Here "war" is less important a term than the objective (goal) of instigating a type of conflict through a cyber attack. And "cyber attack" in the lexicon of the Department of Defense is referred to as an offensive cyber operation. Once the objective has been decided upon, a decision-maker can begin to determine what tools are necessary to achieve that objective. If an objective is sufficiently limited, it can be accomplished with a single tool. It is the achievement of that objective that generates utility.

CHAPTER 7

Defining the Role of Intelligence in Cyberspace

> If ignorant both of your enemy and yourself, you are certain to be in peril.
> Sun Tzu

INFORMATION IS THE LIFEBLOOD of modern states. Intelligence is increasingly facilitating information superiority through an understanding of the cyber domain. The Department of Defense's "Joint Vision 2020" establishes the goal of information superiority on the battlefield. This information superiority enables decision superiority and favorably tilts the strategic and tactical balance. Information superiority is built on cyber power, scale and complexity of attacks, robustness of defense, policy positions, systemic vulnerabilities and dependencies, and actor anonymity and attribution issues. Intelligence plays a mission critical role in assessing these characteristics. The discussion below examines the role of intelligence in identifying these characteristics within the cyber domain and examines how it influences the decision-making of policy-makers. Specifically the focus hones in on how intelligence increases the effectiveness of identifying potential attackers within the cyber domain and informs the decision-making of policy-makers when engaging in covert cyber action directed against a potential adversary. The discussion is designed to serve as a strategic framework in which to understand the role of intelligence within the cyber domain.

Is it really necessary to examine the role of intelligence within the cyber domain as contextually different than in a conventional domain? The short answer is yes. Cyber necessitates independent examination because it is characteristically different, and yet at the same time it is a pervasive feature affecting outcomes within other domains. What differentiates cyber from land, sea, air, and space are three fundamental attributes relevant to intelligence practitioners. First, the cyber domain is a man-made domain. Second, military capabilities across the other domains are managed through the cyber domain. Third, military and civilian aspects of the cyber domain are often intertwined and difficult to differentiate. These attributes pose unique opportunities and problems for intelligence officials.

The man-made nature of the cyber domain makes it a largely virtual domain with its value corresponding to the speed and volume of information contained

within it. However, the cyber domain is not entirely virtual and has numerous real-world connection points to everything from industrial control systems of power and water management facilities to the weapon systems of drones flying above distant battlefields.

Cyberspace is not tangible in the same way as more conventional domains and therefore necessitates a new form of dynamic intelligence evolving from all-source collection of conventional and novel intelligence sources. A recent National Research Council report states that intelligence in the cyber domain is useful for both strategic and tactical purposes.[1] The strategic and tactical importance of intelligence's role in influencing the cyber domain falls within the concept of all-source intelligence. Loch Johnson defines all-source intelligence as one of the fundamental propositions of a theory of strategic intelligence.[2] More importantly for the purposes of understanding the operational and political environments within which offensive and defensive actions in cyberspace can occur, it is necessary to understand what intelligence is within decisions regarding the cyber domain and how intelligence influences those decisions.

DEFINING INTELLIGENCE

There are dozens of different definitions of intelligence, each of which is in some way applicable to understanding cyber action. One of the more succinct and conceptually ordered comes from Michael Warner, who defines intelligence as a "secret, state activity to understand or influence foreign entities."[3] His definition establishes the fundamental premises of both collection and analysis, while including actions designed to influence. Intelligence is vital to the cyber domain because foreign entities are increasingly storing, managing, and directing their governmental, public, private, and military functions in a digitized world.

The traditional intelligence collection types (INTs) are still of immense value, yet they must be combined with aspects of the digitized target spectrum to provide a holistic view of both threats and opportunities. At present the majority of studies in the public domain have focused on defense.[4] This defensive posture is made clear by General Keith Alexander, the director of the National Security Agency and commander of United States Cyber Command, when he writes: "US Cyber Command's efforts and planning aim to ensure that the DoD has done all it can to defend and deter determined adversaries, mitigate dangerous threats, and address nagging vulnerabilities, so that even our most capable opponents will know that interfering with our nation's equities in cyberspace is a losing proposition."[5]

This defensive and deterrent-reliant posture is limiting and prone to inadequacies. Echoing Machiavelli and to some extent Sun Tzu, the adage "the best defense is a good offense" offers a novel way of considering action and intelli-

gence within cyber. More accurately, it allows for a systematic approach to both national cyber defensive and offensive resource allocations. Beyond the efficiency argument for shifting the focus from solely defense to a balance between defense and offense, intelligence collection can help to inform offensive strategies and the decision to use cyber as a weapon. The role of intelligence within cyber becomes increasingly important when considering the difficulty of achieving any significant measure of deterrence within the cyber domain.[6]

The defensive orientation of the majority of cyber literature has a constraining effect on decision-making processes for the use of offensive cyber weapons. This defensive focus is largely due to both the alarmist calls of some scholars and policy-makers and an information communications technologies industry orientation offering many more strategies for defense than for offense. While I do not dispute the need for defense, this defensive focus leads the national security establishment down a path of attempting to create an impenetrable system. If there is one thing that is abundantly clear in the cyber domain it is that the only impenetrable system is the one that has not been made. Cyber is based on physics and algorithms. The mathematics and science behind security measures can be immensely complex and take massive computing power to penetrate, but that does not make them impenetrable. Even the most robust systems secured with checks and encryptions are still highly vulnerable to their users' ignorance or malice, as was the case with Edward Snowden in 2013.

Instead of focusing on a solely carte blanche defensive posture toward cyber security, intelligence can provide both an offensive and defensive picture more effective at safeguarding national security. Taking a step back from the conventional cyber security literature, intelligence can direct cyber security efforts to not merely safeguard national security but also provide an offensive tool for use against other states. The vast literature on intelligence, ranging from the way intelligence influences the policy-making process to how it helps to understand aspects of the development of utility for actions, serves as a guide in defining the role of intelligence within the cyber domain.

Reflecting on Warner's definition of intelligence, the spectrum of intelligence collection methods—from human intelligence (HUMINT) to the more technical collection methods of signals intelligence (SIGINT), measurement and signatures intelligence (MASINT), geospatial intelligence (GEOINT), and open source intelligence (OSINT)—works together in an all-source environment to provide an accurate understanding of foreign entities. (Table 7.1 provides a quick definitional reference for the various intelligence collection types.) The understanding provided by intelligence has largely focused on the conventional domains and on political decision-making. However, as decisions in conventional domains increasingly migrate toward cyberspace, and the systems controlling the tools used in these domains increasingly become digitally connected, the

TABLE 7.1 Intelligence Collection Methods

Intelligence Source Type	Definition
Open Source (OSINT)	Overtly available information found, selected, and acquired from publicly available source.
Measurement and Signatures (MASINT)	Intelligence detected and classified from targets that identify or describe signatures (distinctive characteristics) of fixed or dynamic target sources.
Human (HUMINT)	Intelligence collected through interpersonal contact via human collection officers.
Geospatial (GEOINT)*	The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information.
Signals (SIGINT)	Intelligence collection by interception of signals through various communications technologies.
Cyber (CYBERINT)†	Obtaining prior knowledge of threats and vulnerabilities to information communications systems through a variety of technical means. Also referred to as cyber exploitation (CE).

Source: Definitions are largely adapted from Lowenthal, *Intelligence*.

* U.S. Code Title 10, §467.

† Based on P. Williams, Shimeal, and Dunlevy, "Intelligence Analysis for Internet Security." CYBERINT is considered independent of traditional SIGINT. However, as in many of the other types of intelligence collection, techniques and agencies often overlap.

importance of understanding the technical schematics and decision processes becomes vital to national security.

Nick Cullather, in an article on digital connections on the battlefield, indicates significant advances in the development of network-centric warfare. Cullather notes that the rise of a "revolution in military affairs" has largely not been matched by the intelligence community's ability to keep up.[7] This is of particular importance when looking beyond the network-centric battlefield of conventional weapons to the new zone of confrontation within cyberspace itself. Similarly, Michael Herman finds that counterterrorism intelligence analysis requires a broad spectrum of information sources brought together.[8] ICT facilitates the mitigation of "stovepipes" and increases the efficiency in information transference.[9] Information transmission has also been facilitated following the Intelligence Reform and Terrorism Prevention Act of 2004 by the creation of "fusion centers."[10] ICT has a role to play not only in the conduct of war on the battlefield, but also in the management of a conventional traditional threat spectrum within the fusion centers and beyond in the wider intelligence community.

Terrorism is not commonly regarded as part of the conventional threat spectrum, yet in reality most terrorist acts take place in the physical world and require bombs and guns. However, the information coordination necessary to organize, plan, and conduct warfare, terrorist acts, and political strategies has largely shifted to cyberspace. The 2008 Mumbai terrorist attacks are a poignant example of terrorists leveraging technology and open source intelligence collected from public sites and software such as Google Earth to plan and orchestrate mass murder.[11] As horrific as the use of digital tools for planning attacks is, it is not isolated to open source intelligence collection via tools. Terrorists also use open source cryptography and crypto-currencies to finance their operations.[12] Intelligence agencies are in a competition with other states and organizations to leverage tools effectively to prevent attacks by terrorists and to mitigate international incidents before they arise.

While open source research is fundamentally more powerful than ever before, available open source information provides only a limited aperture to realistically size up threats and targets within cyberspace itself. The problem of intelligence in cyberspace is massive both in terms of scale and complexity of data. Joel Brenner, a former inspector general of the National Security Agency and head of U.S. counterintelligence, indicated there has been an enormous threat emanating from within cyberspace that is not being adequately addressed.[13]

Modern warfare, command and control warfare (C2W), is network centric. Large swaths of the national critical infrastructures in states that pose conventional security and economic threats to the United States are controlled by digital systems. The literature is less focused on the need for understanding these vulnerabilities than it is on safeguarding them. The defensive focus, to a large degree, overshadows the development of offensive capabilities.

Phil Williams, Timothy Shimeal, and Casey Dunlevy make a well-reasoned case arguing for focused intelligence efforts on identifying threats to national cyber security.[14] These authors make a valid point that needs to be addressed and is being addressed by several national strategy documents on the topic, including the *National Strategy to Secure Cyberspace* and the "International Strategy for Cyberspace." One report of particular importance addressing many of the issues brought up by Williams, Shimeal, and Dunlevy is the October 2011 report by the Office of the National Counterintelligence Executive on cyber espionage.[15] A broad spectrum of federal strategies and reports has made identification and protection against vulnerabilities a top priority. More recently the president of the United States under Executive Order 13636 in February 2013 directed the government to begin actively seeking out and planning strategies to mitigate cyber threats to national critical infrastructure.

This is a process that is under way and includes an alphabet soup of agencies from across the civilian and military spectrum of the government. A re-

current problem that keeps cropping up in many of the discussions on critical infrastructure is network awareness. Many companies and firms affiliated with critical infrastructure do not have an adequate understanding of their own vulnerabilities, let alone how they interact to create systemic threats. One industry based on personal communications and working experience that seems to be working very hard to address these issues is the U.S. financial sector, which in many ways is pioneering cyber security efforts under E.O. 13636.

Currently most cyber security is based on attacks or incidents in progress or that have already occurred. It is difficult, if not impossible, to defend against an unknown attack. Much of the effort in the United States cyber community now seems to be equivalent to plugging the holes in the dike after it floods. It is a fact that most cyber attacks are repeat attacks originating at the lower end of the threat spectrum, making the strategy of filling holes in the dike an absolute necessity in an effort to prevent repeat intrusions from identical or similar malware types. Yet this post hoc strategy largely fails to address the more serious problem of accurately anticipating what the next type of attack is going to be. This strategy, best referred to as a "Maginot Line" strategy, is prone to failure in areas where technological and strategic capabilities rapidly evolve. The real challenge is to develop intelligence-based approaches to cyberspace that prevent future attacks before they happen.

There is a significant and sustained effort underway on the defensive side of the cyber debate within the DoD to develop better security. The DoD is currently employing at least three categories of defensive teams to facilitate DoD network protection: DoD information network operations teams (DoDIN Ops), defensive cyber operations–internal defensive measures teams (DCO-IDM or cyber protection teams), and defensive cyber operations–response action teams (DCO-RA or national mission teams).[16] Yet all of these teams are heavily reliant on intelligence on the cyber environment for defense (ICE-D). The teams that fit into these categories are tasked with segments of the overall problem. While the DoDIN-Ops teams are tasked with ensuring sustained secure operations on DoD networks, they are not focused on adversary behaviors in those networks. Their work is informed by adversary behaviors but seeks to maintain network security in aggregate. DCO-IDM or cyber protection teams function as hunter killers within the network. They are tasked with seeking out individuals engaging DoD networks illegally and stopping the attacks or exploits. DCO-RA or national mission teams are tasked with responding to adversary behavior in DoD networks. As should be readily apparent, the problem is enormous and relies on intelligence for all aspects of ICE-D functions. The DoD network environment alone is composed of millions of computing devices and users.

Because we exist in a world of known unknowns and unknown unknowns, to paraphrase Secretary Rumsfeld, cyber security is likely the former rather than

the latter.[17] How can intelligence be used to improve the cyber security situation not only to protect the national infrastructure in a more systematic and logical manner but also to use this information to inform the decision-making processes of policy-makers?

One problem associated with the U.S. cyber community is proximity. Because the community develops, tests, and employs its own tools, it is unable to take into account methods of testing that have not yet threatened systems in the past. This is an in-the-box, out-of-the-box, forget-the-box problem. The designers of systems, software, and networks are talented and smart individuals; they lead the world in technical innovation, yet because they are inside their own systems, it becomes it intrinsically difficult to isolate unforeseen problems. United States Cyber Command and various other teams from the services and the various academies have tried to address this problem by creating competitive cyber teams that compete with one other and against civilian competitors in various challenges such as DefCon capture the flag contests and others. These various DCO and DoDIN-Ops teams also engage one another to consistently foster novel thinking on security.

Yet the challenge is immense, and solutions are best achieved by constant introspection. Below are several proposed strategies to help facilitate the development of improved defensive operations. First, the current orientation toward plugging holes must continue. While this post hoc process is frustrating, it prevents or at least slows further intrusions. The mentality of these DoDIN-Ops is one of defense. The objective is to secure and defend systems against all possible or known types of attacks. The most realistic approach is to defend against known types of attacks. The systems become fortified against repeat incidents or at least can minimize their severity. The work of these teams is not sexy; it is not offense oriented; it is a process of continuous network security development. Second, DCO-IDM teams must also actively hunt in government and defense networks for potential adversaries and leverage information gained through all source intelligence collection and communication with DoDIN-Ops, DCO-RA, and OCO teams to anticipate potential blind spots. These teams must also be regularly rotated to provide them time to think like attackers. Third, DCO-RA teams must leverage all-source intelligence and continuous communications with DCO-IDM and OCO teams to engage adversaries in a defensive posture on foreign networks before they endanger DoD networks. While these teams are in the process of getting organized and established, it is important that these teams have clear interteam communications to mitigate stovepiping. The co-location or consistent rotation of team members would likely facilitate enhanced operational results. The co-location and coordination of members within a team should be of paramount importance as it allows analysts and technicians the opportunity to collaborate and developed a detailed and synergistic understanding of capabilities.

The wider intelligence community must use all-source methods to collect as much intelligence on potential opponents as possible. This means profiling every aspect of other nations' cyber offensive and defensive capabilities. This requires a robust all-source collection methodology. Signals intelligence must look for transmissions and communications as well as spikes in Internet traffic and geo-locate them using IP addresses. These geo-located IP addresses need to be analyzed using satellites and drones to provide accurate geospatial information on the areas in question. Open source intelligence collection should attempt to gain as much publically available information as possible on areas of interest through legal means. Once all of this information has been compiled and assessed, targeted HUMINT operations should begin working on developing assets within these areas or with connections to these areas. These agents should be recruited for multiple purposes. First, they should be used to secure intelligence on the capabilities of potential adversaries. These capabilities are defined in more detail below. Second, agents should also be recruited to become potential insider threats, a tool of particular importance on air-gapped systems.[18] Third, intelligence agencies should also place an emphasis on cyber exploitation (CE) and attempt to probe and map out network infrastructures, vulnerabilities, and strengths of adversaries. The last point is of importance both from an offensive and defensive strategic orientation.

Another major problem with the cyber domain arises out of its systemic complexity. As Williams, Shimeal, and Dunlevy accurately note, cyber defenders often do not have a realistic or accurate picture of their own systems, let alone the systems of adversaries who are attacking them.[19] Following their recommendations, the national security community would be prudent to make use of the principle of knowing yourself. This requires a consistent focus on domestic systems. However, only focusing on domestic systems leads to the "Maginot Line" tendency in which it is assumed networks are created to be impenetrable.

INTELLIGENCE AND THE CYBER BATTLESPACE

The cyber domain is a modern battlespace and necessitates a holistic understanding. To defend against or engage in offensive actions, it is necessary to have an accurate understanding of the operational environment. According to Edward Waltz, any battlespace, whether offensive or defensive, requires a combination of dominant battlespace awareness (DBA) and dominant battlespace knowledge (DBK).[20] The process of identifying what is and is not important to understanding a particular battlespace largely falls to the discretion of policy-makers within the intelligence cycle.

In writing about intelligence and decision-making, Stephen Marrin states: "the intelligence cycle starts with decision-maker information requirements lev-

ied on intelligence collection capabilities, the processing of collected raw intelligence and transmission of this processed material to analysts who decipher its meaning, and relay that understanding back to the decision-makers."[21]

The decision-maker engages in tasking through a number of different "pull" mechanisms including governmental reports, hearings before Congress, presidential directives, and executive orders. These tasking methods and others combine to facilitate within the intelligence community an accurate understanding of what constitutes the battlespace in the eyes of the policy-maker. Often the planning and direction can be informal requests from the executive or from Congress, and at other times it can come from official strategy documents.

Prior to 9/11, terrorism was a priority, but the planning and direction of resources had not yet reached a critical mass sufficient to prevent the terrible attacks on the World Trade Center and the Pentagon. Marrin and others find the intelligence process frequently fails to adequately define what constitutes a tasking priority for the intelligence community, necessitating a "push" from within the community outward. There are many instances in which policy-makers ignore, misinterpret, or misuse intelligence despite adequate tasking and intelligence production and dissemination.[22]

The push mechanism of the intelligence community can happen in several ways. Often it can follow what constructivists call "norm entrepreneurs." Entrepreneurs in the cyber domain include Richard Clarke, or John Arquilla and David Ronfeldt, among others.[23] These individuals bring to national policy-makers' attention issues of importance and help direct the intelligence community's efforts. If, however, they make outlandish claims and statements, their push for new norms can have a backlash and inspire counter-entrepreneurs such as Thomas Rid, who writes that cyber war does not and will not occur.[24] Most traditional intelligence push comes from within the intelligence community itself.[25] Because the intelligence community is pushing intelligence not requested by the decision-makers, the concept of the intelligence cycle can, as Marrin notes, become linear.[26]

Because the domain is so complex, it is beneficial for the president and policy-makers to have individuals with the requisite understanding of the domain not only in policy and legal terms but also in technical terms. The position currently established is known as the cyber czar. While this position is typically filled by someone with policy or legal expertise, it is beneficial for that individual to have a wide background and a reasonable technical understanding so he or she can facilitate complex discussions. Former cyber czar Melissa Hathaway would be a prime example of the type of individual who could accurately convey the complexity of the technical and historical attributes of interactions in the domain while at the same time have a firm grasp on the policy and legal implications of future actions. This person then sits at the choke point of the

push and pull on the cyber domain and distills the information into a balanced reality applicable for decision-makers.

For intelligence to adequately focus its sights on any battlespace, planning and direction from policy-makers must occur. Once policy-makers have established the importance of a battlespace, the intelligence community must find ways to deliver accurate and reliable intelligence. The objective of intelligence collection is not solely to provide real-time information on the battlespace; rather, it is best thought of as battlespace preparation or what Waltz refers to as "intelligence preparation of the battlespace" (IPB).[27] Although Waltz specifically refers to IPB in the context of coordinated conventional warfare and the use of information operations in network-centric warfare, the theoretical principles apply across all domains. IPB, according to Waltz, includes providing an understanding of the "physical, political, electronic, cyber, and other dimensions of the battlespace."[28] Alan D. Campen and Douglas H. Dearth reiterate the concept of IPB in *Cyberwar 3.0*. They state that information warfare requires an accurate knowledge of the battlespace as well as real-time awareness of situations within the battlespace as they arise.

Before moving directly into how each collection type can add to a holistic picture of the battlespace, it is necessary to define what constitutes the battlespace in the cyber domain. The battlespace, according to Waltz, constitutes "all decision-relevant elements within a defined battlespace, and the ability to predict with very high confidence near-term enemy actions and outcomes."[29] More specifically this requires an understanding of human, material, and technical capabilities and the relationship of these capabilities within themselves and to other aspects of the operational environment. It is also important to understand the political implications of alterations in capabilities and the environment over time. A battlespace for cyber can be domestic or foreign and is considered to constitute three basic layers: physical, logical, and social layers. Intelligence must inform policy-makers on all three categories.

The physical layer is composed of a geographical location and the physical devices that constitute the environment. These devices can include hardware such as computers, switches, and routers. The devices that compose the physical layer can also include computing devices such as mobile phones, cars, airplanes, and ships. The physical layer also includes those devices used to facilitate cyber actions such as transoceanic cables, power stations, and buildings. Knowing the physical attributes of a target is often important when attempting to create cyber-kinetic responses. The physical structure of a network can provide clues as to the purpose of the network or point to vulnerabilities of constituent components of a network.

Built upon the physical layer is a logical layer, which makes many of the aspects of the physical layer function. Firmware and software combine to form

a logical layer. Just as there are numerous components to the physical layer there are hundreds if not thousands of different software and firmware applications that combine to make cyberspace function. When targeting a system it is often necessary to have intelligence on the attributes of the system being attacked. A piece of malware designed for a Windows 7 OS zero-day vulnerability will not work if that malware is deployed to a computer running Mac OS X Yosemite.

Lastly, the combination of the physical and the logical layers make the social layer possible. Even if the network and the software layers are air-gapped and highly secure, the social layer, the layer where people interact with the computing device, can still offer up vulnerabilities, as was illustrated in the Stuxnet incident. Knowing who is using a device and how they perceive and interact with the world around them can open up a variety of vulnerabilities including social engineering and phishing. The social layer is composed of both the actual people and personalities using the computing devices and the cyber persona of the individual using a platform.

Aggregating outward, the layers of cyberspace and their attributes in the vernacular of international relations constitute capabilities. Capabilities can be broadly defined as including mechanisms of offensive and defensive military strength such as size and number of offensive cyber units. Capabilities can include doctrinal measures or indicators such as official cyber security and warfare doctrines and can include the size and complexity of systems and their connections to other systems of importance. And capabilities can include technical capabilities such as programming skill within the environment.

The capabilities matrix included below is overly simplified, yet it indicates a host of areas where the intelligence community can provide significant assistance to decision-makers. What is important to consider is that these capabilities are not limited to the United States or its allies. Capabilities need to be assessed on a nation-by-nation basis and on a substate basis as well. These and many other unmentioned cyber capabilities combine to provide an accurate picture of the battlespace.

Identifying the capabilities and political situation of a new battlespace is difficult under the best of circumstances. Cyber is immensely complicated and therefore necessitates a logical template within which to examine capabilities. There is a need for a differentiation between the domestic (defensive) and the foreign (offensive) battlespace. This distinction is important both for tasking and decision-making. When the two battlespaces are separated, they are able to inform one another. Table 7.2 highlights many of the primary areas for consideration within the two battlespaces necessary for DBA and DBK.

The INTs above can and should be focused on these and related areas within the cyber domain. A holistic picture of the above components of the domain will

TABLE 7.2 Components of Cyber DBA and DBK

Domestic (Defense Oriented)	Foreign (Offense Oriented)
Policy considerations (offensive & defensive)	Policy considerations (offensive & defensive)
Domestic network mapping	Foreign network mapping
Budget allocations	Budget allocations
ICT collaboration (alliances, partnerships)	Offensive unit size & training
Defensive unit size & training	Defensive unit size & training
Critical infrastructure	Critical infrastructure
Insider threats for defensive purposes	Insider threats for offensive purposes
Threat spectrum capabilities	Historical record of attack and defense
Known vulnerabilities	Threat spectrum capabilities
Time to attack recognition	Known vulnerabilities
Time to attack attribution	ICT collaborations (alliances, partnerships
Systemic dependencies	Time to attack recognition
Monitoring	Time to attack attribution
	Systemic dependencies
	Surveillance
	Reconnaissance

provide decision-makers with a clearer visualization of the battlespace. Again, following Waltz, a visualization of any battlespace includes the following:

1. Developing a clear understanding of the state with relation to the enemy and environment.
2. Envisioning a desired goal or objective representing the successful completion of the mission.
3. Visualization of the sequence of activities that move the current state to the desired state.[30]

Edward Amoroso argues the intelligence community should focus on creating an addition to the conventional intelligence briefs that consist solely of information pertaining to cyber.[31] Amoroso indicates such a report should focus on current security posture, top and new security risks, automated metrics, and human interpretation. Amoroso's case for the creation of a cyber-specific intelligence brief is sound and works toward promoting an accurate and realistic understanding of the threats and opportunities within this new and evolving domain relevant to national security.

POLICY CONSIDERATIONS

The Joint Chiefs of Staff have placed an increasing emphasis on the cyber domain within various joint doctrine publications. Joint doctrines provide insight into the needs of the services and policy-makers in the employment of and defense against cyber attacks. Documents also include many of the ways cyber

has come to rely heavily on intelligence assets. Information superiority has become a mission critical aspect of defending national security. The Department of Defense's "Joint Doctrine for Command and Control Warfare" dating back to 1996 highlights the importance of intelligence products in support of C2W. The document indicates the use of intelligence assists in the conceptualization of all aspects of a battlespace.

Comprehension of any battlespace, including the cyber domain, requires understanding the policy environment in which an action occurs. Is there a national cyber defense strategy within the targeted country? How have they publicly or privately declared they would respond to hostile acts within the cyber domain? An example of the policy environment can be found in the "Department of Defense Strategy for Operating in Cyberspace." The strategy outlines five strategic initiatives in its declassified report:

Strategic Initiative 1: Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential

Strategic Initiative 2: Employ new defense operating concepts to protect DoD networks and systems

Strategic Initiative 3: Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy

Strategic Initiative 4: Build robust relationships with U.S. allies and international partners to strengthen collective cyber security

Strategic Initiative 5: Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation

The recently declassified sections of the report cited in the media indicate a doctrinal shift in the way the DoD approaches the cyber domain. The *Wall Street Journal* reports that DoD sources as early as 2011 indicated that some instances of cyber attacks can constitute an act of war.[32] This has further developed as recently as September 2014 with the NATO pledge for mutual defense in the event of significant cyber attacks that might result in the invocation of Article 5.[33] When asked what constitutes an act of war in cyberspace that would rise to a level that would result in the successful invocation of Article 5 for mutual defense, NATO secretary general Rasmussen said that the goal was to achieve "strategic ambiguity" to keep adversaries guessing and to act as "ambiguous deterrence."[34]

Although the current position on what constitutes an act of war in cyberspace within the eyes of the United States and NATO remains uncertain, understanding the policy positions within the domestic battlespace and in the foreign battlespace helps alleviate information asymmetries and establish clearly identifiable patterns for response. Whether it is the knowledge that Germany and the Netherlands both have official cyber security doctrines or that China has begun implementing a policy of making offensive cyber capabilities a strategic priority,

the overt and covert collection of policy positions provides policy-makers with a foundation for understanding intelligence related to cyber.

Policy platforms also help to codify international law, to create zones of norms or an identifiable policy framework in which states will interact or respond to incidents emanating from cyberspace.[35] While both the United States and Russia have made known a cyber attack could constitute an act of war, there has been little elaboration on specific characteristics of such an attack within the official policy-making circles of government. Often states will intentionally leave room for policy ambiguity as a mechanism of deterrence.[36] Understanding ambiguity, information gaps, and information asymmetry is crucial particularly in comprehending how leaders arrive at decisions. As in conventional warfare, in cyber conflict the minimization of or the knowledge about what a potential adversary will do in a given situation provides a strategic edge. Although there has been little in the form of codified policy delineation on what level of cyber attack would constitute an act of war, the academic community has been heavily engaged in attempting to apply existing legal frameworks to the cyber domain. The most notable work in this arena is the *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which works through in rigorous detail how actions within cyberspace could fall within existing international law.[37] Yet as rigorous as the work is, there is no single government required to adhere to its findings on the applicability of international law, and even within the laws themselves there was a significant amount of debate as to what constituted various levels of action in cyberspace. Instead of thinking of sponsored academic works such as the *Tallinn Manual* as clear policies to which states should adhere, they should be instead thought of as roadmaps to guide states in developing policies.

CE—NETWORK MAPPING, SYSTEMIC DEPENDENCIES, AND HISTORICAL RECORDS

Understanding the policy environment both domestically and among foreign adversaries is only part of the larger intelligence process. Cyber exploitation (CE) constitutes a series of technological and analytical approaches to cyber-specific espionage. CE for the purposes of conventional intelligence collection can include the penetration of foreign networks to secure information on weapons systems, policy positions, and much more. CE is invasive yet does not disrupt, deny, or destroy data; it collects data. When CE operations focus intelligence on the cyber domain for offensive and defensive purposes, the objective is to understand the systems themselves. The goal becomes identifying the strengths and weaknesses of systems, the connectivity of systems to points of interests, and the interaction of those systems with strategic and tactical objectives.

There are numerous methods of CE; for the purposes of simplicity only a few are examined here. Network mapping is a form of CE that studies the physical connectivity of networks or the availability of insecure ports. This type of mapping provides information on what types of systems and servers operate on different networks and identifies the characteristics of the various component parts these systems constitute. Network mapping can drill down to very low levels on particular networks and provide significant information speed and types of hardware on various networks. This information can also be used to isolate portions of networks to identify potential heavy traffic users or other sources of potential exploitation.

Network mapping is also useful for illustrating the potential for any particular targeted attack to extend beyond its intended target and result in collateral damage or blowback. Conceptually network mapping is not dissimilar from attempting to map radar or surface-to-air missile locations prior to a bombing campaign. The intent of network mapping is to gain an operational knowledge of an adversary's systems prior to engaging in an OCO.

Forensic analysis of the Stuxnet worm found the worm partially employed network mapping to target its attacks, focusing on isolated networks using memory sticks as the initial method of transmission.[38] Once in, Stuxnet focused its attack on networks with programmable logic controllers (PLCs) of a specific type and caused uranium enrichment centrifuges to malfunction.[39] The level of sophistication required to drill down to get to this level of detail to plan an attack is remarkable, particularly considering the complexity and number of overall systems and the air-gapped nature of the systems.

Network mapping is both an offensive and defensive intelligence endeavor. To adequately prepare both the defensive and offensive battlespaces, an accurate picture of systems is needed. Arguably the dual domestic-foreign pictures are complementary and help avoid violating part 2.13 of Executive Order 12333, which prevents any covert action from influencing U.S. political processes, public opinion, policies, media, or various sections of the Foreign Intelligence Surveillance Act.[40]

Network mapping and monitoring is a double-edged sword. Legally network mapping can be considered CE, and therefore domestic network mapping by U.S. intelligence agencies without a warrant would be prohibited. However, network mapping is of critical importance to the maintenance of national security infrastructures. Thus far the intelligence community does not have a formal commitment from the White House or the Justice Department to engage in any domestic CE operations.[41] Currently in the United States there is an uneasy and inefficient public-private commitment to providing information on network security across critical infrastructure. A thorough understanding of domestic and foreign networks assists in visualization for both offensive and defensive

purposes, and effort to push reasoned analysis of threats has begun to make its way into Congress.[42]

Network mapping assists in the identification of network components. Once network components are known, it becomes necessary to explore vulnerabilities within systems. Most damaging are zero-day vulnerabilities, which are vulnerabilities in computer applications of which even system administrators are unaware. The Stuxnet attack exposed several zero-day vulnerabilities in the Windows software controlling/monitoring the programmable logic controllers, causing the attached centrifuges to spin outside of their safe operational standards.

Systemic vulnerabilities necessitate a thorough understanding of the historical record of different types of attacks and exploits. The identification of zero-day vulnerabilities should lead network administrators to immediately patch these gaps. Intelligence plays a role in identifying what types of attacks have been used in the past and what vulnerabilities these attacks attempted to exploit. Historical accounting is important for both offensive and defensive preparation of the battlespace. For obvious reasons it is important to prevent repeat attacks on domestic systems; at the same time it is important not to engage in repeat attack methods once a vulnerability on an opposing system has been fixed. Such an attack would likely be ineffective and lead to anonymity-attribution problems.

The historical accounting of attack types by countries and substate actors also alerts operators within the intelligence and military community to the threat spectrum capabilities of a particular cyber adversary. Understanding the threat spectrum capabilities of states facilitates an accurate conceptualization of their power to operate within the domain. Table 7.3 is a representation of known threat spectrum capabilities.

The above areas of consideration within CE are only a small sampling of the overall tasking priorities for intelligence using CE methods. They hint at a broad applicability for CYBERINT methods in the preparation of the battlespace.

CONVENTIONAL INTELLIGENCE

Intelligence collected on budgetary allocations, offensive and defensive cyber unit sizes, and training methodologies provides the clearest parallel to conventional intelligence. As in conventional intelligence, most countries are frequently unwilling to release data on absolute military expenditures or the sizes and force structures within their military. Military capabilities are a closely guarded secret in most countries. Capabilities are particularly secretive in the cyber domain. Often if cyber capabilities are exposed, they cease to be capabilities.[43] Once Stuxnet was discovered by the Iranians, defensive measures were taken to "plug" the holes the Stuxnet attack employed. This dramatically reduces

TABLE 7.3 Cyber Threat Spectrum

Levels (Types) of Attack	Description	Feasibility	Complexity
Propaganda	The propagation of information via the Internet to affect public, private, or governmental opinion. This can be combined with web vandalism.	High	Low
Web Vandalism	The defacement of official or private websites for nonpolitical or political purposes.		
Denial of Service Attack (DoS)	The denial of service to a user or users of a computer, server, website, network, or system.		
Distributed Denial of Service Attack (DDoS)	The denial of service to a user or users of a computer, server, website, network, or system—this type of attack is similar to a DoS attack but is distributed across a botnet or other computer systems remotely activated.		
Cyber Exploitation	The secret collection and reproduction of digital data from computers or networks.		
Equipment Disruption	The disruption or interception of communications or information flow from systems.		
Critical Infrastructure	The targeted disruption of systems designed to provide for or maintain critical infrastructures of vital importance—systems include power, water, fuel, communications, commercial, and transportation.		
Compromised Hardware Systems	The implantation of malware designed to affect systems in the production phase of a product.		
This is not an all-inclusive threat spectrum.		Low	High

the effect a repeat Stuxnet attack would have on any other nation. Whereas missiles can be launched with repeated success because the ability to defend against a moving projectile is difficult, a similar cyber weapon is more easily defended against once it has been identified. Antivirus software can be reprogrammed to identify and isolate repeat threats, and zero-day vulnerabilities can be patched.

An excellent example of an open source analysis of cyber capabilities comes from Stokes, Lin, and Hsiao, who examine in explicit detail the construction, location, leadership, and mission of many aspects of the Chinese People's Liberation Army information warfare programs.[44] Their report is an example of a high-value detailed analysis that could be supplemented by conventional intelligence to enhance policy-maker and combatant commander comprehension of the battlespace. The detailed analysis of the location and force structure can cause an enemy to shift its tactics, techniques, and procedures (TTPs) and make them less reliable. Alternatively, not revealing that information has been gained on TTPs can provide an offensive edge in cyber operations.

The implications for conventional intelligence collection methods indicate that intelligence on cyber does not necessarily need to remain cyberbound or exclusively within the realm of CE. Many metrics such as force size matter in cyber and can be examined to create a better assessment of potential adversaries. Cyber force size is particularly important from a malware development perspective. Complex coding scripts typically necessitate large numbers of programmers to develop and test the scripts. The ability for an individual to accomplish highly complex attacks is possible but less likely than a large cyber warfare unit working with the same objective.

Likewise, knowing where a unit is located or how programmers were trained can help planners determine the best response to a particular attack, or how best to manipulate their organizational structure. Derek Clark and Kai Konrad refer to this as identifying the weakest link.[45] The identification of the weakest link is particularly important in cyber defense and offense. There are multiple fronts (systems) needing defense. All it takes is one "best shot" to achieve significant damage. While this weakest link can be identified through CE operations outlined in the previous section, it can also be identified within the training, command, and organizational structure of units charged with conducting or protecting against cyber attacks.

Closely related to the conventional military metrics above, yet likely unique to the cyber domain, are public-private ICT collaborations. Although most countries have programs for military public and private collaborations with universities and businesses for research and development, within the cyber domain the importance of this relationship is magnified for multiple reasons. First, much of the training and education necessary to conduct offensive or defensive oper-

ations within cyberspace can be learned at public institutions or can be crafted for private sector use. This extends far beyond the development of technology to the actual training of the warfighter, the development of the platforms upon which the domain rests, and more. Second, these collaborations spread out but do not diffuse potential vulnerabilities.

Because collaborations can form the foundational aspects of the cyber warriors within offensive and defensive units, they can train, equip, and prepare in ways far different from conventional military means. Most countries have a balance between civilian and military protection of their national cyber infrastructures based largely on the development of computer emergency response teams (CERTs). An intelligence assessment of the strength and quality of ICT collaborations is of critical importance in understanding the cyber battlespace.

ICT collaborations are not necessarily official and do not need to be highly structured and regimented. Alexander Klimburg provides evidence Russia and China have created groups of plausibly deniable cyber attackers.[46] Creating an accurate open source measure of unofficial collaborations is difficult. An intelligence focus on unofficial collaborations with entities can contextualize cyber incidents such as the 2007 cyber attacks directed at Estonian governmental, bank, and communications websites.[47] The attacks were motivated by a decision to move a Russian war memorial from central Tallinn. While initial reports indicated Russia was the culprit, Russia denied any participation in the cyber attacks.[48] The reality is somewhat murkier and more akin to an unofficial sanction or condoning of cyber attacks by the Russian government.[49]

The collection and production of intelligence on more conventional attributes of pertinence to the cyber domain is a role in which the intelligence community is likely already engaged. Occasionally reports on issues relating to this category of intelligence are published for public consumption. A recent report of this type was produced for the U.S.-China Economic and Security Review Commission to examine China's capability to conduct cyber warfare and cyber exploitation.[50] Knowledge of capabilities is still applicable to the cyber domain and is greatly influenced by conventional intelligence collection methods and subsequent analysis, which contextualizes the meaning of raw intelligence.

HUMINT AND CYBER

Human intelligence (HUMINT) stands out in cyber for two particular reasons. First, HUMINT agents can provide accurate internal information on systems and access to those systems unavailable through CE and other intelligence collection methods. Second, human assets can serve as a bridge between the external world and air-gapped or other forms of secure networks. As was indicated above, it is likely that the Stuxnet virus was distributed using a thumb drive,

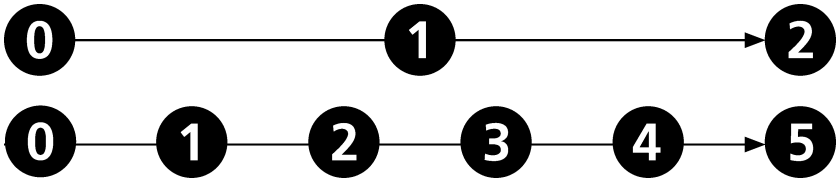
which needed to be inserted into a machine within an air-gapped network. HUMINT agents can serve as a vulnerability against which most network administrators will be unable to provide significant protection.

The role of a HUMINT asset with access to information on networks can be extremely damaging. Even if the agent is on a lightly classified network, the repercussions of his or her actions can be enormous. The scandal caused by Bradley Manning (now named Chelsea Manning) leaking more than 260,000 diplomatic cables to WikiLeaks in 2010 is illustrative of the problem posed by internal threats.[51] Manning's leak and the even more damaging 2013 document releases by Edward Snowden, a former employee of a contractor affiliated with both the NSA and CIA, highlight the potential damage a rogue employee can have on the ability of the intelligence community to keep information secret.[52] Snowden's insider collection and subsequent release of documents pertaining to the National Security Agency likely constitutes one of the most significant intelligence leaks of all time and resulted in an estimated 1.7 million documents being released in violation of U.S. classification law.[53] Moreover, unlike the leaks by Manning, the Snowden leaks revealed many of the TTPs used by the NSA in its intelligence operations in the cyber domain. These revelations have been extremely damaging and have resulted in changes in the way adversaries safeguard their cyber infrastructure.

HUMINT threats need to be developed and enhanced for offensive intelligence and protected against for domestic national security counterintelligence. Gaining access to the technical schematics, documents, information, login procedures, or any of a multitude of other targets of intelligence a HUMINT asset could provide is a critical aspect added directly by intelligence to the understanding of the cyber domain. Furthermore, HUMINT agents are almost impossible to detect under normal circumstances as they can often engage in significant espionage while still easily performing the normal duties. Unlike the spy thriller days of old when agents had to sneak out of a building with classified documents in a folder or a box, they can often place thousands or millions of documents on a solid-state drive and easily conceal it upon exiting a facility. Many of these drives are smaller in size than a penny.

Beyond the collection of intelligence from HUMINT sources, these insiders can assist in the implementation of cyber actions. Information within a 2005 report by the U.S. Secret Service in cooperation with Carnegie Mellon indicated that up to 29 percent of all attacks against a surveyed group of critical infrastructure stakeholders were initiated by insiders.[54] The majority of motivations behind these attacks were not related to intelligence or covert action. This, however, does not preclude the possibility of using insiders to affect or gain information or access on adversary systems. The recruitment and maintenance of insider threats by the intelligence community should be a top priority. These

FIGURE 7.1 Timeline for Attack Implementation



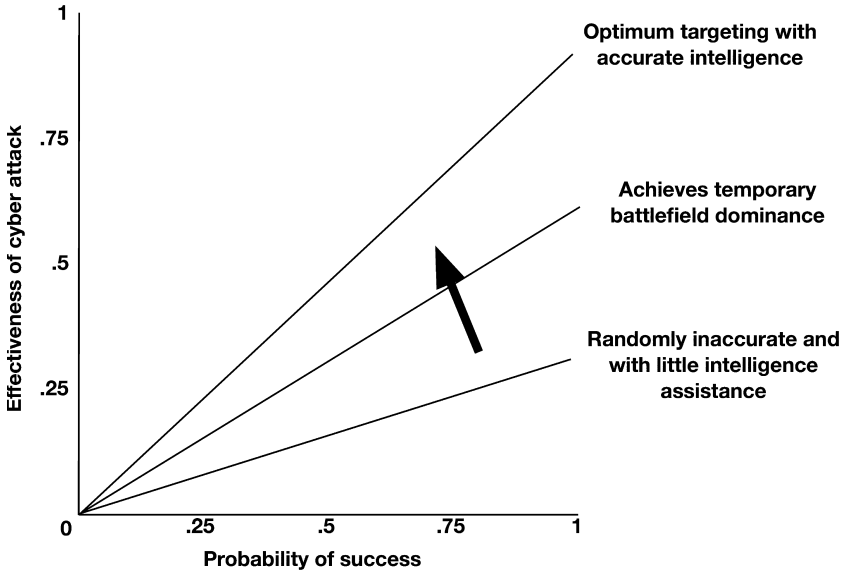
agents can offer a mission a critical component, often during times when more lengthy intelligence collection processes are constrained by events.

TIME FOR ATTACK RECOGNITION, COMPLETION, AND ATTRIBUTION

Attack recognition and attribution are also critical for both a defensive and offensive battlespace planning. All of the intelligence collection methods and the focus of the intel process of trying to comprehend the cyber domain culminate in understanding, from a mission critical orientation, the progression of cyber attacks. Figure 7.1 is a simplified model for understanding attack planning and progression within a battlespace modeled loosely on the JP 3-51 electronic warfare-planning model.[55] This model is informed by intelligence collection. Line one of the figure indicates a policy-maker's perspective on the process of engaging in conflict. A conflict initiation is (0) planned, (1) implemented, and (2) completed. Policy-makers want to know what resources any given action will take and how long it will take to complete it. In cyber a more accurate timeline for action in cyberspace requires (0) intelligence collection, (1) operational planning of the attack with an informed knowledge of the battlespace, (2) understanding of the time it takes for the attack to be completed, (3) how long until the attack is recognized as an attack by the adversary, (4) how long until that adversary can do something about the attack, (5) how long until the adversary assigns attribution for the attack. The ordering of the items listed above greatly affects the ability for an attack to be conducted successfully. Intelligence informs the policy-maker and commander as to the feasibility of a particular type of attack and the probability of success. If recognition of an attack occurs early in the timeline of events the probability of success is diminished.

The timeline can be tested in much the same way conventional weapons are tested. It would be absurd to send a bomber over a potential target with a completely untested bomb, or to send a soldier into battle with an untested model of rifle. Just as weapons are tested in the physical world, they need to be tested in the cyber domain as well. This testing provides added information to both

FIGURE 7.2 The Influence of Intelligence on Cyber Operations



Modified from E. Waltz, *Information Warfare*.

the policy-maker and the combatant commander as to the effectiveness of the weapon and the timeline of events above. If a cyber weapon is slow and easily detectable, its probability for success is diminished. This lowered probability for success does not nullify its use but does condition it.

One aspect of this phase of IPB is that it is extremely beneficial to both the offensive and defensive strategic and tactical operations. By planning and testing potential attacks against theoretical adversarial systems, the intelligence community provides an out-of-the-box perspective necessary to prevent similar attacks against domestic targets. This logic would indicate an attempt to use a worm like Stuxnet against the U.S. infrastructure would run into greater problems than if the weapon had been developed first elsewhere.

IPB AND ITS IMPACT ON CYBER

The role of intelligence in cyber is not dissimilar from its role in the conventional domains. There are new areas in which collection and analysis need to occur, yet its overall objective remains the same. Returning to Edward Waltz's concept of information preparation of the battlefield, figure 7.2 illustrates intelligence's influence on operations originating within the cyber domain. The role of intelligence in cyber is to accurately facilitate an understanding of those

entities and the possible tools by which to influence them. The cyber domain is surrounded with hype and hysteria. Many of the claims are accurately based in reality. But the known unknowns are still enormous within this evolving domain, and it is incumbent on intelligence to provide an accurate assessment of the current state of affairs.

All-source intelligence for cyber operations requires the intelligence community to think beyond domestic system defense. The focus should be balanced between foreign and domestic intelligence, thereby mutually informing one another and creating a systemic defense for national assets in addition to better facilitating decision-makers with a more accurate picture of how a potential cyber attack might succeed or fail.

CYBER AS COVERT ACTION

To further define the role of intelligence in cyber, it is necessary to look more deeply into the laws codifying the conduct of the intelligence community. All of the above sections provide a framework for defining the role of intelligence with regard to IPB. Cyber conflict is, by its very nature, covert. Even if an attack is discovered, it is often unattributable. Attacks can be designed to go unnoticed and affect changes to systems and their components for days, weeks, or months without detection. Even in instances where groups such as Anonymous publically take credit for attacks, responsibility is typically claimed post hoc. Nearly all examples of state-on-state cyber attacks have been covert.

The covert nature of cyber brings full circle Warner's definition of intelligence as attempting to influence. Covert action is a secret operation to influence a foreign entity. At least in theory, most, if not all, cyber attacks begin covertly. Section 1.7(a)(4) of Executive Order 12333 regarding intelligence activities describes covert action:

> Conduct convert action activities approved by the President. No agency except the Central Intelligence Agency (or the Armed Forces of the United States in time of war declared by the Congress or during any period covered by a report from the President to the Congress consistent with the War Powers Resolution, Public Law 93-148) may conduct any covert action activity unless the President determines that another agency is more likely to achieve a particular objective.[56]

Evident in the early structuring of the governmental approach to cyberspace is the categorization of cyber operations as covert actions. The Department of Defense originally took the lead with General Keith Alexander as the head of both NSA and Cyber Command, a path that has continued now that Admiral Michael Rogers has taken over as the head of both organizations. This indicates the president has established an agency other than the Central Intelligence

Agency as the primary covert operator within this domain. While the logic behind having a military intelligence organization commander and an organizational structure that falls under the U.S. Strategic Command (STRATCOM) runs counter to EO 12333, the institutional capacity of the DoD in the technical domain and the scale of the problem being faced within this new domain make the assignment appropriate.

SUMMARIZING THE ROLE OF INTELLIGENCE WITHIN THE CYBER DOMAIN

In defining the role of intelligence within the cyber domain, it is necessary to take a holistic approach. From a collection perspective, the intelligence community should be and has been working in coordination with a hybrid push-and-pull intelligence cycle to both elevate the importance of this domain and facilitate collection within it. The emphasis has been heavily defensive up to this point and largely focused on countering threats rather than anticipating them. This needs to change, and the only way this can change is if the intelligence community begins to actively turn its sights on adversaries and develop more rigorous all-source intelligence combining novel CYBERINT technologies to augment reporting on this domain. Parroting Amoroso's assertion, cyber should be included on the daily intelligence briefs of policy-makers. The inclusion would likely start the process of demystification of this immensely complicated domain.

Cyberspace is a domain that can be used to fulfill all aspects of Warner's definition of intelligence to some degree. It is a domain in which it is possible to gain understanding about other states beyond and within the domain itself, but it is also a domain that can influence other states' policy decisions as well as perceptions. In particular, accurate intelligence on both sides of the domestic-foreign divide can mutually inform decision-makers about vulnerabilities and the eventual decision to use cyber as an offensive weapon or how best to defend against attacks. Moreover, intelligence can rein in the debate on cyber to a more realistic area of operations predicated on sound estimates rather than on grandiose speculation.

The intelligence community itself commonly is the point of origin for OCOs emanating from the cyber domain and will likely serve as a force multiplier in instances where a combined conventional cyber attack is necessary. To engage in cyber conflict, just as in conventional conflict, intelligence is needed to prepare the battlespace and facilitate an accurate assessment of the probability for success and utility for any type of operation. This preparation hones the weapons, decisions, and effect of a potential operation. More importantly for national security, a thorough and accurate preparation of both the foreign and domestic battlespaces will serve to inform and enhance cyber security.

CHAPTER 8

How Actors Decide to Use Cyber—a Rational Choice Approach

> Man is a rational animal—so at least I have been told. Throughout a long life I have looked diligently for evidence in favor of this statement but so far I have not had the good fortune to come across it.
>
> Bertrand Russell, *An Outline of Intellectual Rubbish*

ARE STATES RATIONAL ACTORS in cyberspace? The evidence presented in this chapter builds on the arguments and data established from previous chapters and provides substantial evidence indicating that states are behaving rationally in cyberspace. The rational behavior of states provides a substantial framework upon which to build future models for deterrence as well as within which to predict state actions in cyberspace. As with any rational model deficiencies, however, the balance of evidence presented below is clear: states engage in cyber operations with an expectation of positive utility.

Rationality is predicated on assumptions. These assumptions, when applied beyond the domain of pure economic theory, pose philosophical problems. To apply rationality it is necessary to assume the world is simpler than it actually is. This simplification or theoretical conceptualization of the world helps to explain on an aggregate level how things work. Social science is complex. To understand how and why people, nations, and states behave it is necessary to simplify the world through the construction of theories. Absent a parsimonious theory, social scientific analysis devolves into a causal mess. Theories allow us to focus on those aspects of social interactions that best enhance our understanding of the world. Not every theory is correct, and in truth all social scientific theory must necessarily be falsifiable. By theorizing that actors behave rationally when engaging one another in cyberspace operations, the argument advanced is parsimonious, testable, and falsifiable. As interactions in the cyber domain increase between states, a foundational understanding of state behavior in this domain becomes increasingly important.

Using the rational choice framework the analysis below hones in on the cyber decision-making model in four steps. First, what is rationality? Second, how do

risk and uncertainty play a role in decisions? Third, what is the model for bilateral expected utility of cyber conflict? Lastly, this chapter concludes by applying the model against data on cyber incidents. Although largely composed of formal model development and testing, the analysis here serves the vital purpose of establishing the logical framework for rational decisions in cyberspace.

RATIONALITY

Rationality is a common concept in both economics and international relations, and it is not necessary to reinvent the wheel. This book uses John Von Neumann and Oscar Morgenstern's fundamental characteristics of rationality:

1. Completeness—for any two simple lotteries A and B, a choice must be either
2. $A \geq B$ or $A \leq B$ (or both).
3. Transitivity—for any three lotteries A, B, C, if $A \geq B$ and $B \geq C$, then $A \geq C$.[1]

Although there are other more detailed aspects that can be added to the above definition of rationality, those are the two central assumptions, which constitute the foundation of utility theory as explained by Bruce Bueno de Mesquita. Bueno de Mesquita states utility theory essentially comprises the following aspects:[2]

1. Individual decision-makers order alternatives in terms of their preferences;
2. The order of preferences is transitive so that if A is preferred to B and B p C (where p is to be read as "is preferred to") then A p C;
3. Individuals know the intensity of their preferences, with that intensity of preference being known as utility;
4. Individuals consider alternative means of achieving desirable ends in terms of the product of the probability of achieving alternative outcomes and the utility associated with those outcomes; and
5. Decision-makers, being rational, always select the strategy that yields the highest expected utility.[3]

Rationality is essentially consistent across decision-making models. There are forms of bounded or conditional rationality, which limit the information available to actors; however, within these models the basic tenets expressed above are consistent. Whether a rational choice is being made in conventional warfare, diplomatic negotiations, or cyber conflict, the core assumptions of rationality remain the same.

As with any formal model there are several necessary assumptions: First, decision-makers are regarded as a unitary single actor. This principle, illustrated in the first chapter and in several subsequent chapters, is necessary to avoid Arrow's impossibility theory, which states that when three or more distinct options

are available, no community-wide system can convert the ranked preferences of individuals (multiple) into an aggregate—complete and transitive—rank order.[4]

Because of a focus on a unitary actor decision-maker, this model is confined to those entities that employ a single unitary decision-maker on matters relating to the instigation of cyber attacks. This eliminates groups such as Anonymous, which function as collective decision-making entities and do not fulfill the requirements of rationality. Groups that do not function with a unitary decision-maker likely cannot be examined as rational actors, and therefore the utility construction of these actors would serve little ultimate purpose.

Second, preference orderings are able to incorporate aspects relevant to the cyber domain. Just as conventional conflict can incorporate variable factors defining the value of options for a given choice, the cyber variable can also influence the value of potential options within a given decision.

Third, a common misperception is that value for preferences of an actor instigating conflict must be related to the values assigned by the target of a conflict initiation. Such an understanding would indicate two states engaging in a conflict both have an identical understanding of the ex-ante choice. Intersubjective valuations of utility are not dependent, as this would violate Arrow's theorem. A decision, whether overt or covert, is predicated on the preferences of the individual actor, not on the dyad. Both actors must independently consider conflict initiation rational for conflict to occur.

These considerations are not unique to the cyber domain, but they are highlighted here to preempt misunderstandings about the decision-making model. The rational choice for an actor is predicated on the utility of the options available. The actor then creates a rank order model based on the value of each option. This choice functions independently of the utility construction of options for a potential opponent. A divergence in the utility calculations between the potential parties to a conflict is best referred to as an information asymmetry and is one of James D. Fearon's rationalist explanations for war.

Embedded within a rational choice are the concepts of uncertainty and risk, which here are calculated, not cognitive functions associated with any rational choice. The next section focuses on how these two terms are applicable to cyber decisions.

UNCERTAINTY AND RISK

Uncertainty and risk both play a role in the ability of a decision-maker to arrive at an ultimate decision as to whether or not to engage in conflict. Although Bruce Bueno de Mesquita uses a measure of coalition cohesiveness within a nation's geopolitical region, such a tool is not applicable within the cyber framework for several reasons. Bueno de Mesquita establishes that states are uncer-

tain about the likely response of other nations to the instigation of conflict.[5] First, as discussed, alliances and coalitions are not of clear importance to decisions made regarding the instigation of conflict within cyberspace. Second, a constraint imposed on a geopolitical region would be inappropriate as the regional delineations of the cyber domain make geopolitical delineations untenable when examined from the physical layer of cyberspace. Uncertainty is difficult to comprehend within the cyber domain and functions within a system of systems environment across the physical, logical, and social layers of cyberspace.

Uncertainty occurs when a decision must be made in the absence of objective or subjective probability values attached to alternative outcomes. Because this is an emerging field of study and there is no immediately logical measure of uncertainty within the cyber domain, it is necessary to assume states making decisions within cyber are doing so based on objective epistemological foundations. Unlike in conventional conflict where epistemological limits are best isolated in the complexities of alliances, within the cyber domain the limits of knowledge are a function of anonymity. Being discovered in the act of a cyber attack influences the certainty or uncertainty of a probability of success for a given cyber operation. Anonymity is examined in two unique contexts, both of which influence the risk behavior of a state. Using anonymity as a measure of uncertainty and risk is a significant theoretical departure from Bueno de Mesquita's conceptualization of uncertainty.

Anonymity influences the probability of success and is therefore included as a factor influencing decisions to engage in cyber operations. Anonymity also influences the expectation of the changes demanded should a state lose in bilateral conflict. A state with greater certainty of its anonymity is less likely to fear losing and is therefore more risk acceptant. Within the rational model to engage in offensive cyber operations, it is assumed that as the probability of maintaining anonymity decreases, the effect of a loss of anonymity on the perception of what might be lost increases. Because uncertainty is embedded into the utility calculation in the form of a measure of effect, risk and uncertainty are combined into a single measure. Uncertainty represents the ability to maintain the effect of anonymity on the perception of what might be lost. A state that is risk averse is less willing to take a risk on any form of loss. As the potential for loss increases, a risk-averse state becomes less willing to instigate conflict. A state with a high degree of anonymity has a low degree of uncertainty and vice versa. This uncertainty is measured at two points in time, at time to and $t\text{o} \rightarrow t + n$. Time $t\text{o} \rightarrow t + n$ is indicative of the time at which an attack is completed. Because anonymity is measured using a hazard function model, it is possible to derive two different probabilities at two different points in time. Because anonymity changes over time, the certainty of its effect changes as well.

At the outset of attacks most actors should find their level of certainty of maintaining anonymity quite high. Anonymity should be high at the point of conflict initiation because anonymity interacts with the probability of success. This certainty diminishes as the attack progresses. This is akin to estimating that alliances at the beginning of a conflict are likely to alter as a conflict proceeds. Whereas Bueno de Mesquita's model relies on a single-point estimate of certainty based on cohesiveness of the alliance ex-ante, this measure is more accurate as it evolves and can be defined at both the point of conflict initiation and at a future point in time deemed sufficient for the successful completion of an operation. In conventional conflict, it would be reflected as alliances shifting over the duration of a conflict. In cyberspace, alliances don't have the same importance; therefore it indicates a change in the certainty of states' expectations of loss in a conflict as a given attack proceeds toward completion.

Risk-acceptant actors are more likely to decide to attack even in an increasingly uncertain environment than are risk-averse actors. Risk-averse actors are less likely to decide to attack as uncertainty increases. Both of these factors influence the ultimate decision to attack. However, unlike in Bueno de Mesquita's model, uncertainty has a direct effect on the overall utility function of states deciding to attack within cyber.

UTILITY THEORY OF (CYBER) CONFLICT

The construction of utility theory for cyber conflict at its aggregated level functions no differently than the construction of utility for any type of decision. Truthfully, Bueno de Mesquita's development of an expected utility theory for international conflict is robust and can be applied with modifications to nearly any political decision. Below, the entirety of his expected utility theory is laid out to facilitate the discussion and development of a cyber-specific model.

Bueno de Mesquita states in his work that utility can be estimated as a "random walk" between +1 and –1 or a difference between perfect agreement in policy positions ranging to a complete divergence in policy positions.[6] This represents, as noted by Bueno de Mesquita, a bounded range for utility. The boundedness of utility in economics is a reflection of diminishing marginal utility reaching a point at which value ceases to increase.

The theory of boundedness has been examined in detail by Bernoulli, Von Neumann and Morgenstern, Fishburn, and others. Though it is possible to have an unbounded utility function, in the political context of what Quiggin refers to as a rank-dependent expected utility (RDEU) model, the issue of diminishing marginal utility of value is revealed.[7] Contextually, here it is reasonable to assume that once two states perfectly align in policy positions (+1), there is noth-

ing to be gained—indicating actions to achieve additional utility from such a situation would be inefficient. Similarly, once two states are at their maximum divergence in policy positions (–1), there is nothing more that can be lost. Note that loss and gain in this context do not indicate the possibility to shift an opposing state's policy position, but rather indicate the distances on a policy spectrum between the two states.

Policy positions for this model are measured using Strezhnev and Voeten's data derived from the United Nations General Assembly.[8] They create a measure of affinity based on what percentage of votes each country agreed on. Within their coding, abstention represents a half agreement. This gives a score between 1 and 0. This book assumes that .5 represents a midpoint in policy affinity between two states and sets .5 at 0. The resultant number is then multiplied by 2 to give a proportional distance to 1. Because this proportional distance is inverted, the proportional distance is multiplied by –1. This provides a standardized score of vote difference within the United Nations General Assembly during a given year ranging from 1 to –1, with 0 as the midpoint. This measure is used to estimate the potential utility to be gained from engaging in offensive cyber operations with another state at its maximum, ignoring anonymity and probability for success.

The conventional expected utility model for international conflict identifies seven types of nations, each having an effect on the calculations about the instigation of international conflict.

Included in the cyber decision-making model:

1. The potential initiator (hereafter called *i*);
2. The potential defender (hereafter called *j*);

Not included in the cyber decision-making model:

3. Those nations with policies viewed by *i* as friendly toward *i*, but not toward *j* (hereafter called k_1);
4. Those nations with policies viewed by *i* as friendly toward *j*, but not toward *i* (hereafter called k_2);
5. Those nations with policies viewed by *i* as friendly toward both *i* and *j* (hereafter called k_3);
6. Those nations whose policies are viewed by *i* as neither friendly toward *i* nor toward *j*, but as friendly toward other third parties (hereafter called k_4);
7. Nonaligned nations with policies viewed by *i*, as neither friendly toward *i*, nor toward *j*, nor toward other states (hereafter called k_5).[9]

Bueno De Mesquita asserts that when a leader contemplates the expected utility of the initiation of conflict, the following variables are significant:

1. The relative strength of *i* and *j*;
2. The value *i* places on changing *j*'s policies to be more in line with its own preferences, relative to the possible changes in policy *i* might be forced to accept if it loses to *j*; and
3. The relative strength and perceived policy interests of all k_1, k_2, k_3, k_4, *and* k_5 (as seen through the eyes of *i*) that might intervene in the ensuing conflict.[10]

Bueno De Mesquita defines the component aspects of the utility for the instigation of bilateral conflict as follows:

$E(U_i)b$ = *i's* = *i's* expected utility for the instigation of bilateral hostilities
U_{ii} = *i's* utility for *i's* own policies is by definition $U_{ii} = 1$.
U_{ij} = *i's* utility for j's policies. This can vary between +1 and –1.
$(U_{ii} - U_{ij})$*t*o = *i's* perception of what might be gained by succeeding in a bilateral conflict with *j* in which *i* can then impose new policies on *j*.
$(U_{ij} - U_{ii})$*t*o = *i's* perception of what might be lost by failing in a bilateral contest with *j* in which *j* can then impose new policies on *i*.
P_i = *i's* current perception of its probability of succeeding against *j* in bilateral conflict.
$1 - P_i$ = *i's* current perception of its probability of losing against *j* in bilateral conflict.
$\Delta(U_{ii} - U_{ij})_{t0 \to t+n}$ = *i*'s perception of anticipated change in the difference between *i's* policies and *j's* policies over the period *t*o (the present) to some future time (*t* + *n*).
$\Delta(U_{ij} - U_{ii})_{t0 \to t+n}$ = *i's* perception of anticipated change in how much *j* would want to alter *i's* policies in the future compared to *j's* current perceived policy differences with *i*.[11]

Based on the above components, Bueno de Mesquita indicates,[12] and this holds true for cyberspace as well as any other political decision, that *i* believes *j* is moving closer in regard to policy positions, therefore indicating an improvement in relations between the two nations if

$$\Delta(U_{ii} - U_{ij})_{t0 \to t+n} < 0$$

Such a change as in conventional conflict might alleviate or minimize the potential need to engage in any type of operation. However, this also indicates the reverse is true.[13]

$$\Delta(U_{ii} - U_{ij})_{t0 \to t+n} > 0$$

When *i* believes *j* is moving further away relative to the policy position as indicated above, this indicates deterioration in relations and will likely increase the probability of conflict. The improvement or deterioration in relative policy posi-

tions over time can either enhance or mitigate the drive to conflict. This principle illustrated by Bueno de Mesquita is not unique to conventional conflict. An appropriate example would be the 2007 cyber attacks against Estonia. It is conceivable that if the policy position of the Estonian government had been one of shifting toward closer relations with the Russian Federation, the likelihood of attacks would have been diminished. The reality was that the change in policy positions was increasingly divergent, and the result was a large cyber incident.

Just as relative policy positions over time are important in influencing the utility of any potential conflict, the probability of success in conflict is also important to influencing the utility of engaging in conflict. The probability of success in conflict is largely determined by a measure such as power (capabilities) to achieve one's stated goals, as was examined in chapter 4. This power score can be ascertained as a function of material capabilities or other determinants. Bueno De Mesquita[14] represents the probability function for conventional conflict as

$$8.1 \qquad P_i = \frac{cap_{ij}}{cap_{ij} + cap_{jj}}$$

Where *cap* (Capabilities) for Bueno de Mesquita represents

$$8.2 \qquad Adjusted\ Capabilites = composite\ capabilities^{\log[(miles/miles\ per\ day)+10-e]}$$

Capabilities are constructed using CINC scores from Singer and Small 1977 and a representation of the debilitating effect distance has on conventional capabilities.[15]

Because actions occurring within cyber are unique in composition and application from conventional methods of conflict as examined by Bueno de Mesquita, they must contain constraining assumptions different from those of conventional conflict. Although Bueno de Mesquita identifies three combinations of potential combatants as present in cyber, it is only reasonable to consider one.[16]

a. conflicts between nonaligned states;
b. conflicts between aligned states; and
c. conflicts between nonaligned and aligned states;

As has been discussed in previous chapters, cyber attacks require anonymity to be successful. In a situation of anonymity it is not logical to assess the alignment of states, as such an alignment would likely only come to full fruition for the benefit of either party after the success or failure of a potential attack. Therefore, a cyber attack on a state that is aligned is unlikely to be different than an attack on a state that is unaligned. If there is any doubt on this issue, historical precedence should suffice to explain.

In 2007 the cyber attacks conducted against Estonia, an aligned nation within NATO, should have indicated a combined strength of alliances sufficient

to thwart the decision process of any potential attack initiator. The combined power scores of the alliance are substantial. Yet not only did the alliance fail to recognize the attack as an act constituting an alliance response, but its entire response was muted or absent.

The same processes can be seen in the instances of other attacks ranging from the Israeli attack on Syrian nuclear facilities to the attacks of Stuxnet on Natanz. Although the latter was likely created through national collaboration, the measure of alliances associated with each country likely had little to no effect on the outcome of the attack. It is therefore unreasonable to consider any form of alliance in the present modeling of decisions within cyber as having any significant influence. This therefore leads us to assumption 1:

ASSUMPTION 1: In cyber conflict alliances are of little or no importance, as they fail to affect either the conduct or the success of a potential attack within the cyber domain.

This assumption is consistent with the reality of the cyber domain and attacks occurring within it. If, however, cyber attacks are used as force multipliers, it is best to combine their utility function with the conventional utility formulas including alliances as indicated by Bueno de Mesquita.

While the utility formula for bilateral conflict can function adequately for virtually any decision process in international relations, the probability for success must be contextually tailored. Although it could be tailored to account for diplomatic negotiations as well as conventional military operations, this work, as was developed in chapters 4 and 5, illustrated a way in which it can be adapted to the cyber domain. This adaptation leads to a set of cyber specific assumptions on capabilities:

ASSUMPTION 2: Capabilities in the cyber domain are not the equivalent of capabilities in other more conventional domains of interaction. Cyber capabilities are constructed by a measure of theoretical capabilities interacting with demonstrated capabilities, scaled by a measure of national digital dependence. These capabilities are not dependent on distance, as interactions within the cyber domain are almost instantaneous and suffer no loss of effectiveness as their distance from origin increases.

Assumption 2 is predicated on works related to cyber security and development ranging from Kramer, Starr, and Wentz to Nye, Betz and Stevens, and others.[17] Cyberspace operations do not have the same capability characteristics as conventional conflict. Cyber operations require a unique set of variables to explain capabilities within this domain and a unique comprehension of these capabilities independent of conventional forms of conflict.

Below are the variables developed in previous chapters:

Variable Name	Variable Code
Military unit designation*	MUD
Legal and regulatory frameworks*	LRF
Economic and social context*	ESC
Technological infrastructure*	TI
Industrial application*	IA
Military budget allocation*	MBA
Threat spectrum capabilities	TSC
National digital vulnerability	NDV

*indicates weighted variables

These variables combine to create the cyber capability model below in equation 8.3.

$$8.3 \quad Cyber\ \ Power = \frac{(MUD + LRF + ESC + TI + IA + MBA)\ TSC}{NDV}$$

The above indexed variable is simplified to where F represents theoretical cyber force capabilities, T represents demonstrated threat spectrum capabilities, and D represents national digital dependence.

$$8.4 \quad Cyber\ \ Power(capabilities) = \frac{F\ T}{D}$$

Despite a reconceptualization of capabilities into terms relevant for cyberspace, the probability for success or P_i, success in cyber is not solely dependent on cyber capabilities, as conventional conflict is on conventional capabilities. As illustrated in chapter 5, anonymity plays a vital role in determining the success of any potential attack within the cyber domain. This leads to assumption 3:

> ASSUMPTION 3: Capabilities within the cyber domain must be interacted with a measure of anonymity. Because the cyber domain is a virtual domain controlled by human agents, it has the ability to be turned off and on and to be managed in ways unique to its virtual qualities. Therefore it is necessary to include in the probability of success not only a measure of capabilities between potential adversaries unique to cyber but also a measure for anonymity.

As the ability to maintain anonymity decreases, its effect forces the probability of success toward zero. Anonymity also functions in another way that doesn't merely influence the probability of success in conflict; it influences the perception of the potential loss a state might face. Anonymity is a powerful attribute of cyber operations and heavily influences a cyber decision-making model. Notation for anonymity within the cyber model is represented as follows:

A_i = *i's* perception of its probability for maintaining anonymity.
$1 - A_{i_{t0}}$ = the effect of *i's* perception of its probability for maintaining anonymity.
$1 - A_{i_{t0 \to t+n}}$ = the effect of *i's* perception of its probability for maintaining anonymity at the time of the completion of attack.

As the ability to maintain anonymity increases, its effect approaches zero. This relationship is the inverse in nature. When this number reaches zero, its effect increases. This effect interacts with the perception of what might be lost by failing in a bilateral contest. The best way to conceptualize this term is to think like a criminal. If the chance of being caught for a crime, ceteris paribus, was zero, it is more likely an individual would attempt such a crime regardless of its overall probability of success.

The above two assumptions also lead to the following measure of P_i (*i's* current perception of its probability for success), where *F* represents theoretical force capabilities interacted with *T*, demonstrated threat spectrum capabilities, scaled against *D*, a measure of national digital dependence. P_i for cyber actors is represented in equation 8.5 as

$$8.5 \quad P_i = (A_i)\left(\frac{F_{ij}\ T_{ij} / D_{ij}}{F_{ij}\ T_{ij} / D_{ij} + F_{jj}\ T_{jj} / D_{jj}}\right)$$

This can be simplified to Bueno de Mesquita's notation as

$$8.6 \quad P_i = (A_i)\left(\frac{cap_{ij}}{cap_{ij} + cap_{jj}}\right)$$

Combined, these three assumptions fundamentally change the way in which utility is assessed for cyber operations within the expected utility theory of international conflict. If we recognize that the probability function for the utility of international conflict is different than the one conceived of by Bueno de Mesquita, it is possible to restate the utility function for bilateral cyber conflict initiation from equation 8.7 to reflect both the incorporation of the construction of P_i and the influence of anonymity on a perception of potential loss in equation 8.8.[18]

$$8.7 \quad E(U_i)_b = (P_i(U_{ii} - U_{ij}) + (1 - P_i)(U_{ij} - U_{ii}))_{to} + P_{it0}(\Delta(U_{ii} - U_{ij}))_{t0 \to tn} + (1 - P_i)_{t0}[\Delta(U_{ij} - U_{ii})]_{t0 \to tn}$$

Here Bueno de Mesquita's utility for the initiation of bilateral conflict is modified to include the effect of anonymity on the perception of loss in the present and at a future point in time. This is reflected in the equation 8.8 below:

$$8.8 \quad E(U_i)_b = (P_i(U_{ii} - U_{ij}) + (1 - P_i)[(U_{ij} - U_{ii})(1 - A)])_{to} + P_{it0}(\Delta(U_{ii} - U_{ij}))_{t0 \to tn} + (1 - P_i)_{t0}[(\Delta[(U_{ij} - U_{ii})(1 - A_{it0 \to t+n})]_{t0 \to tn}$$

The general utility function for bilateral conflict as defined by Bueno de Mesquita above in equation 8.7 functions the same way for cyber conflict with only minor modifications seen in equation 8.8. These modifications take into account the influence of anonymity as explained above. Again, it is important to remind the reader that in addition to the visible changes in the structure of the utility formula accounting for the effect of anonymity, the composition of the probability function P_i has been modified to incorporate cyber-specific variables. Although the calculation is fundamentally different, the general utility function is only slightly altered. This change still allows many of Bueno de Mesquita's original propositions to be adapted into a decision-making model for cyber with only modest alterations. What follows are Bueno de Mesquita's propositions modified with language conducive to and incorporating the assumptions of the cyber domain.[19]

PROPOSITION 1: States involved in a purely bilateral conflict cannot rationally attack a more powerful state within the cyber domain, regardless of whether their choice occurs under risk or uncertainty, and regardless of their risk propensity unless they are assured positive utility predicated on anonymity across all three characteristics of anonymity.

Proposition 1 is consistent with most concepts of rational conflict initiation up to the point where anonymity begins to play a role. Bueno de Mesquita notes that this proposition is in line with Organski and Kugler and other scholars of conflict initiation.[20] Although it is consistent with much of the conventional literature on the rational instigation of conflict, it seems to fly in the face of much of the cyber literature on asymmetry. While asymmetry is important, it is important to contend that the power score in cyber is scaled by national digital dependence. If anonymity cannot be maintained indefinitely, ultimate probability of success decreases to zero. This indicates that while the domain is asymmetric, attacks are only rational if (a) there is a preponderance of power, or (b) a state can assure its anonymity so as to prevent retaliatory action.

Just as Bueno de Mesquita notes, this proposition does not preclude the possibility of a state engaging in hostile acts against a more powerful state, even if it can't maintain its anonymity, only that such an act is irrational. Under this proposition it is not possible to include the revealed policy preferences among other states (indicated by Bueno de Mesquita), as those policy preferences are largely irrelevant in coming to the aid in either the instigation of or defense against conflict.

PROPOSITION 2: A risk-acceptant leader calculating expected utility under risk could initiate a cyber conflict against a stronger ally if it is assured a high probability of indefinite anonymity.

This proposition largely flies in the face of conventional wisdom. It is assumed $(U_{ij} - U_{ii})_{t0} = i$'s perception of what might be lost by failing in a bilateral contest with j in which j can then impose new policies on i. However, as was examined above, anonymity can virtually prevent the imposition of j's policies on i if anonymity can be maintained over time. If an attacker never expects to be discovered, even if the attack fails to accomplish its stated goals, such an attack might be conducted with low utility gains because the consequences of failure are virtually nonexistent.

If such attacks are compared to peer-to-peer sharing of movies, music, and other forms of media, it is evident that out of the millions of users only a small number are ever prosecuted for theft of intellectual property. The number is so small as a percentage of the overall number of individuals engaging in theft that it becomes statistically insignificant. Statistical insignificance eliminates meaningful deterrents that prevent individuals from engaging in illegal behavior.

PROPOSITION 3: When $U_{ii} - U_{ij}$ reaches its maximum value (i.e., when $U_{ij} \rightarrow -1$), the probability, given the random walk principle or boundedness, i anticipates that $\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n}$ is negative increases, as does the likelihood that i anticipates that $\Delta(U_{ij} - U_{ii})_{t0 \rightarrow t+n}$ is positive. Under these circumstances, Bueno de Mesquita indicates i is likely to anticipate an improvement in future relations with j.[21] This proposition holds true within the cyber context and can indicate a situation in which even if $E(U_i)_b \geq 0$ as indicated by current values (at $t0$) can be altered to reflect $E(U_i)_b \leq 0$. This alteration is predicated on future expectations and can prevent conflict between two parties.

Cyber conflict decision-making, like conventional conflict decision-making, is based on present and future changes in positions. Although this particular proposition is difficult if not impossible to illustrate using case examples, its proof of concept is logical. It is possible to assume two nations, both hostile to one another, avoiding conflict based on anticipated changes at a future point in time.

PROPOSITION 4: Let $U_{ii} = U_{ij} = 1$, so that $U_{ii} - U_{ij} = 0$. If $U_{ij} = U_{ii}$, then the policies of i and j are, by definition, indistinguishable. Consequently, regardless of whether i is risk acceptant or risk averse, and regardless of whether a decision is being made under risk or uncertainty, in this circumstance, it is always true that $E(U_i) = E(U_i)_b$. Now, by the random walk assumption (discussed above), if $U_{ii} - U_{ij} \rightarrow 0$, it is likely that $\Delta(U_{ii} - U_{ij})_{t0 \rightarrow t+n} \geq 0$ and $\Delta(U_{ij} - U_{ii})_{t0 \rightarrow t+n} < 0$. Since the sign of $E(U_i)_b$ is determined by the magnitude of P_i relative to $1 - P_i$, it follows that, among closest allies, if i is stronger than j, $E(U_i)$ cannot be less than zero, and if i anticipates a deterioration in relations in the future, $E(U_i)$ must be greater than zero. Then, as noted by Bueno de Mesquita, there is a

> paradox. Under these circumstances in any form of conflict, cyber included, when anticipated future changes indicate a decline in relations between two close allies, conflict initiation by the stronger nation should be expected.[22]

The logic of the above proposition is counterintuitive, as is noted by Bueno de Mesquita.[23] Similar behavior arising between allies in the cyber domain has not been documented; however, it stands to hold that in this regard cyber conflict is no different from conventional conflict. The effectiveness of using cyber conflict in this regard, independent of other tools of force, is likely of limited value.

The above propositions indicate, based on the expected utility theory developed, when it is and is not rational to instigate conflict within the cyber domain. The propositions should indicate the differences between conflict initiators and their targets, the likely victor of any given attack, when conflicts are irrational and therefore not necessary, and when the use of cyber is rational.

APPLYING THE EXPECTED UTILITY THEORY OF INTERNATIONAL CYBER CONFLICT

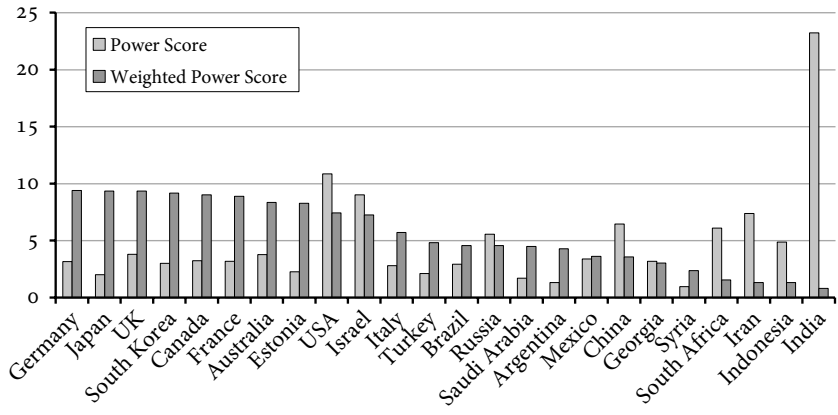
Testing the above propositions is particularly difficult due to data availability on cyber operations. Below the model is applied, and the rationality of state behavior in cyberspace is tested. The model is tested using open source case examples, and each case has been tested in four separate ways in an attempt to illustrate the effect of each of the component aspects of the model. Testing of cases includes (1) static changes in policy over time with the inclusion of a measure of anonymity, (2) dynamic changes in policy over time with the inclusion of a measure of anonymity, (3) static changes in policy over time excluding a measure of anonymity, and (4) dynamic changes in policy over time excluding a measure of anonymity. These four measures are meant to illustrate when it is and is not rational to instigate a cyber attack based on different assumptions.

Figure 8.1 is a rank ordering of the states measured and includes their cyber power score. Note that the power score is separate from anonymity associated with the type of attack employed. The figure clearly illustrates India was an outlier in the unbiased measure of cyber power.

Figure 8.1 includes two power scores. The first is a raw power score based on an equal weighting of all aspects of a state's cyber power. According to this rubric, India would be the most powerful state, followed at a distance by the United States. The question is why would India, a state with a small percentage of its population using the Internet and only moderate scores in all categories, rank so highly in terms of power score?

The basic definition of power score indicates that a state's power is scaled by its vulnerabilities, and this is where India thrives. Because only a small per-

FIGURE 8.1 State Cyber Power Scores (2011)



centage of India's population uses the Internet, its national digital vulnerability is proportionately very low. This measure is deceiving. To correct the measure over the influence of vulnerability, cyber power scores were weighed according to their components. Just as not all weapon systems are equal in conventional conflict, not all aspects of cyber power are equal. The actual weighting of power scores can be found in the appendixes. The weights of the components of cyber power are predicated on a modification of the Economist Intelligence Unit's report on cyber power.[24] The result is that India goes from being one of the most powerful nations because of its low penetration rates of information communications technologies to one of the least powerful states within the sample.

The power scores indicate Germany is the most powerful country overall within cyber space and that the United States comes in a mediocre ninth place. This is not to say that the United States has ineffective military cyber units. If military units were all that mattered, the United States would be at the top of the cyber power rankings with its enormous defense budget. Unlike in conventional conflict where it is possible to protect a nation with sheer offensive power, the cyber domain extends across the military and civilian divide, making it necessary for a powerful state in cyber space to excel in all areas of cyber power. Currently the United States does not excel in all areas and is therefore not as powerful as some of the other nations within the sample. Cyber power requires a combined national effort, and a failing in one area of cyber power can diminish a nation's overall cyber potential.

Although the United States isn't as "powerful" as other nations, this does not mean it doesn't have a sufficient number of potential targets. The next section outlines how states working under the assumption of anonymity can generate

positive utility even against a much more powerful ally. The section looks at the data and attempts to draw preliminary conclusions, based on the evidence presented and not on statistical tests. This is done because often a study will jump right into the statistics without examining the results in the broader context of the individual cases involved. Because this study only has twenty-five cases, it is possible to provide a more in-depth look at the processes occurring.

THE EXPECTED UTILITY OF STATES ACROSS INCIDENTS

This section outlines the utility calculations of twenty-five cases (twenty-three unique) in which two countries were identified as likely participants to a cyber action. These cases are from the Center for Strategic and International Studies (CSIS) report on significant cyber incidents dating back six years. [25] Significance is largely a subjective measure. The CSIS defines "significant" for its cases as "successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars."[26] For the purposes of this study, significance was parsed out to an even more rigorous degree. This analysis includes only successful attacks by governments on other governments and their national security assets. Within this condensed listing, targets must be government agencies or related national critical infrastructure targets. These critical infrastructure targets include targets within the defense industrial base, electric, financial, or radar systems. Disruption of these systems or severe damage or theft occurring to these systems must pass the test of posing a reasonable, clear, and present national security threat.

Policy affinity was measured in the year prior to an attack for the static models and measured as the change policy affinity in the two years prior for the dynamic tests. Prior years are used rather than the current year because vote counts are completed on a yearly basis. The argument presented here leverages assumed anonymity measures predicated on anecdotal evidence, a decision-maker using the hazard model, and the relevant data from chapter 5 would arrive at similar results. The purpose of the discussion is to illustrate that when decision-makers decide to attack, they are acting rationally based on a positive utility score predicated on realistic assumptions. The assumptions for construction of power and the influence of anonymity are unique to the cyber domain and are necessarily included.

Of the twenty-five incidents documented in which two states are identified, the attacking party had a positive utility in every case when anonymity is included in the model. If anonymity is excluded from the model, there are only nine instances in which it would have been rational to engage in hostile activities within the cyber domain. These results provide a cursory story that states appear to be behaving rationally within the assumptions established in previous

TABLE 8.1 Expected Utilities across Incidents

Year	Type	Attribution	Static Policy Change	Static Change Ignoring Anonymity	Dynamic Policy Change	Dynamic Ignoring Anonymity
2006	CE	Undefined	0.87	–1.18	0.87	–1.19
2006	OCO-ED	Undefined	0.28	–0.74	0.28	–0.73
2007	OCO-DDOS	Undefined	0.28	–0.26	0.29	–0.27
2007	CE	Undefined	0.33	–0.72	0.32	–0.69
2007	CE	Undefined	0.32	–0.64	0.32	–0.63
2007	CE	Undefined	0.24	–0.53	0.24	–0.53
2007	OCO-CID	Defined	2.48	2.10	2.41	2.04
2007	CE	Undefined	0.32	–0.64	0.32	–0.63
2007	CE	Undefined	0.38	–0.51	0.39	–0.54
2008	CE	Undefined	0.21	–0.45	0.21	–0.45
2008	CE	Undefined	0.29	0.23	0.30	0.24
2008	OCO-DDoS	Defined	0.55	0.19	0.56	0.20
2009	CE	Undefined	0.37	–0.75	0.37	–0.76
2009	CE	Undefined	0.21	–0.45	0.22	–0.46
2010	CE	Undefined	0.38	0.30	0.34	0.27
2010	OCO-WD	Undefined	0.05	–0.09	0.04	–0.08
2010	CE	Undefined	0.40	–0.70	0.40	–0.71
2010	CE	Undefined	0.38	0.30	0.34	0.27
2010	OCO-CH	Defined	2.77	2.38	2.72	2.33
2010	OCO-CH	Defined	2.27	1.95	2.41	2.07
2011	CE	Undefined	0.43	–0.86	0.42	–0.84
2011	CE	Undefined	0.25	–0.53	0.25	–0.51
2011	CE	Undefined	0.24	–0.52	0.23	–0.50
2011	CE	Defined	2.64	2.20	2.67	2.22
2011	CE	Defined	2.75	2.30	2.68	2.24

CE: cyber exploitation; OCO-ED: equipment disruption; OCO-DDoS: distributed denial of service; OCO-WD: website defacement; OCO-CH: compromised hardware; OCO-CID: critical infrastructure disruption

chapters. Table 8.1 lists the resultant expected utility across the four categories being measured for all incidents. The table also identifies the type of attack and whether there is a certain attribution or an uncertain attribution associated with the attack.

The data in table 8.1 illustrate within the confines of the anonymity assumption that states are rational to engage in OCOs emanating from cyber. It is reasonable, based on the discussions in previous chapters, that the assumption of anonymity is necessary to some degree for any type of significant offensive cyber operation and significant cyber exploitations resulting in significant degradation of capabilities or relative advantage. If the assumption of anonymity is removed, then only nine cases indicate a positive utility for attack. This would indicate that 61 percent of OCOs initiated without the assumption of anonymity were irrational. A high percentage of irrational actors in interstate conflict does not conform

to Bueno de Mesquita's results on the expected utility of international conflict.[27] High levels of irrational behavior can lead to several potential conclusions. First, the number of cases is too small to accurately define whether states act rationally within the cyber domain. Second, there is something about the cyber domain that induces states to act irrationally. Third, states are acting rationally because they assume a degree of anonymity even if that anonymity is not actually present.

Although there are a limited number of cases, the number of cases closely represents the publicly known actual population, indicating that the results accurately reflect the population. If states were acting irrationally, they would have likely suffered the consequences of their losses and been dissuaded from engaging in repeat actions. What is observed, however, is that certain states engage in repeat behavior against multiple different targets and frequently against the same targets. This behavior indicates either a cognitive/psychological issue or that the states are acting on a rational belief of gain. To this point the argument advanced that states are rational actors has largely been supported. Lastly, the decision to engage in OCOs is rational if the actors make even modest assumptions of anonymity prior to engaging in their attacks. When those assumptions are not present or are weak, the only time a state engages in OCOs against another state is when it has an overwhelming cyber power advantage.

The nine cases in which anonymity does not matter have several common characteristics, including a small number of potential hostile actors and a power advantage by the OCO initiator.

Stuxnet and Flame are broken down into four separate incidents represented, as the utility of the United States versus Iran and Israel versus Iran are unique in many ways.[28] The attacking party in both of these incidents had an extreme negative policy affinity with the target and an enormous cyber power advantage. Both of these instances possess significant scale and complexity, resulting in a speedy degradation in the probability of maintaining anonymity. Likewise the Israel-Syria attack of 2007 and the Russian-Georgia attack of 2008 were combined kinetic-cyber attacks diminishing the need for long-term anonymity. This indicates that in six of the nine instances where anonymity was not important over time, the attacker had both a significant power advantage and had little to no need for maintaining indefinite anonymity.

The remaining three incidents in which anonymity was of little importance were China-India attacks. In each of these cases the policy goal was limited, and the attacker always had a positive utility. Although they are close in policy affinity scores, they do not fall neatly in line with *Proposition 4* because in two of the three instances the affinity scores seemed to be growing closer together, while diverging in the third. A source of potential measurement problems is located in the inability of power scores to reflect any shift in relative power over such a short time frame. Each of these incidents was a form of CE and likely poses

methodological problems for a model predicated on significant OCO operations. The operations were possibly conducted because China feared an increase in the relative power of its neighbor, with whom it has had sporadic conflicts over an extended period of time. Although the motivation is unclear, what is clear is that China acted with anonymity in its favor and with a cyber power advantage.

Of the twenty-five incidents examined, only six have a defined attribution. Of those six, all had positive utility across the four types of measurement regardless of anonymity and regardless of changes in policy affinity. Two of the attacks are easily attributable after the fact because they were combined with kinetic operations following the success of the cyber operations. The other four incidents are Flame and Stuxnet, revealed to be a mix of operations between the United States and Israel, which was disclosed through intelligence leaks.[29]

The remaining incidents in which the attacking party remained undefined were identified as probable attacker with no definitive attribution, indicating that at least part of the triad anonymity had been maintained. By maintaining anonymity, states such as China are able to engage in offensive cyber operations against other states with limited fear of retribution. This limited fear of retribution, influenced by anonymity, allows them to attack more powerful states. Often the offensive cyber operations were limited in scale and size; however, the possibility for gain makes such attacks worthwhile.

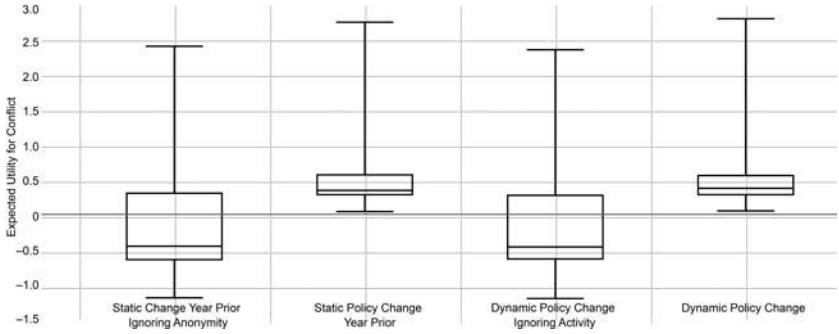
The next section examines how data hold up against the propositions presented above. Each proposition is examined in detail using the available data.

EXAMINING THE PROPOSITIONS

Proposition 1 indicates that states will not engage in cyber conflict if they are at a power disadvantage unless they are assured a moderate to high degree of anonymity across all three dimensions of anonymity. This is illustrated using the data by running t-tests at $a = .05$. The results indicate that when accounting for anonymity in either a dynamic or static policy environment, it is rational to engage in OCOs against opponents. However, when anonymity is excluded, there is no statistical significance associated with the instigation of hostilities. Figure 8.2 illustrates the box plots of the distribution of the utilities for each case within the sample. Table 8.1 includes the hypothesis tests across all four categories of tests.

The results indicate a relationship between positive utility and an assumption of anonymity in the decision to attack. If *Proposition 1* is to hold, it would be unlikely that a state with low anonymity and a relative power disadvantage would engage in hostile activities against another state. There are no available data on cases involving a state with little to no anonymity and a power deficit. This proposition is currently supported by the robustness of the evidence, sug-

FIGURE 8.2 Expected Utilities Box Plot



gesting a relationship between positive utility and anonymity. The lack of cases in which an instigator was at an overall utility disadvantage makes it impossible to make definitive claims on *Proposition 1*. If the assumption that states are rational actors holds across models, then the data would indicate that in most instances states would not have engaged in OCOs in the absence of anonymity.

To further drive home the point about anonymity, there is no evidence of any retaliatory actions by victimized states toward their likely aggressors. This lack of response indicates that most if not all attacks resulted in a degree of victory for the attack instigator.

Proposition 2 builds on *Proposition 1* and indicates that even if a state is at a power disadvantage, it might, given conditions of anonymity, engage in hostile acts against a more powerful state. Although there are no instances in which a state with no assumption of anonymity attacked from a position of relative weakness, the data from table 8.2 seem to support this proposition. If the assumption of anonymity is correct, then it goes a long way toward supporting China's risk-acceptant behavior in attacking other states through the cyber domain, particularly states with a relative power advantage. However, since there is no way to test this assumption, the anecdotal evidence from the data must suffice at present.

Propositions 3 and 4 are interesting because they both propose conditions under which states would be more or less likely to engage in hostilities. To test these propositions it was necessary to examine changes in policy affinity over a defined period of time to see if states were more or less likely to engage in or abstain from hostilities depending on changes in policy preferences. Table 8.3 shows the results of a simple *t*-test on whether changes in policy affinity are statistically significant. The results indicate changes in policy affinity have no bearing on whether a state is more or less likely to engage in hostilities. Although the

TABLE 8.2 Results of *t*-Tests of Utilities

	Static w/ Anonymity	Static w/o Anonymity	Dynamic w/ Anonymity	Dynamic w/o Anonymity
Number of values	25	25	25	25
Minimum	0.05	−1.18	0.04	−1.19
Mean	0.7876	0.0952	0.784	0.0944
Std. Deviation	0.9309	1.131	0.929	1.126
Std. Error	0.1862	0.2262	0.1858	0.2252
One sample *t*-test				
Theoretical mean	0	0	0	0
Actual mean	0.7876	0.0952	0.784	0.0944
Discrepancy	−0.7876	−0.0952	−0.784	−0.0944
95% CI of discrepancy	0.4033	−0.3716	0.4005	−0.3704
	to	to	to	to
	1.172	0.5620	1.167	0.5592
t, df	t=4.230 df=24	t=0.4209 df=24	t=4.220 df=24	t=0.4192 df=24
P value (two-tailed)	0.0003	0.6776	0.0003	0.6788
Significant (alpha=0.05)?	Yes	No	Yes	No

results provide some anecdotal evidence that states are more likely to engage in cyber hostilities when there is a decrease in policy affinity, the relationship is not significant. Figure 8.3 illustrates the distribution of changes in affinity over time and provides a good visualization for where states fall with regard to when they decide to attack in relation to their policy affinities. Of note is that the mean of changes in affinities for states engaging in offensive cyber operations is negative. However, as mentioned above, no statistical inference can be derived.

One other aspect arising out of *Propositions 3 and 4* is the question of whether states are more likely to attack when they have close policy positions or more divergent policy positions. *Proposition 4* indicates that conflict is more likely when states have close affinity because they are concerned more about negative shifts in policy than states that are extremely divergent in policies. This is contrasted with *Proposition 3* indicating that states are less likely to engage in conflict with states that are at the polar opposite end of the policy affinity spectrum because there is only truly room for improvement. Table 8.4 indicates the affinity scores of states in the year prior to attack. This is a static number. The question is whether conflict is more likely between states with close affinity scores or with more divergent affinity scores. In other words, are states with very similar policies more likely to attack one another through the cyber domain than states with dramatically divergent policies? Figure 8.4 illustrates the distribution of the affinity scores around the mean.

The data in table 8.4 do not indicate significance at $a = .05$. The data do indicate significance at $a = .1$. Because this is not the preestablished threshold and

TABLE 8.3 T-Tests of Affinity of State Likelihood of Conflict

Number of values	25
Mean	–0.0072
Std. Deviation	0.05997
Std. Error	0.01199
Lower 95% CI of mean	–0.03195
Upper 95% CI of mean	0.01755
One sample *t*-test	
Theoretical mean	0
Actual mean	–0.0072
Discrepancy	0.0072
95% CI of discrepancy	–0.03195 to 0.01755
t, df	t=0.6003 df=24
P value (two-tailed)	0.5539
Significant (alpha=0.05)?	No

FIGURE 8.3 Distribution of Changes in Affinity over Time

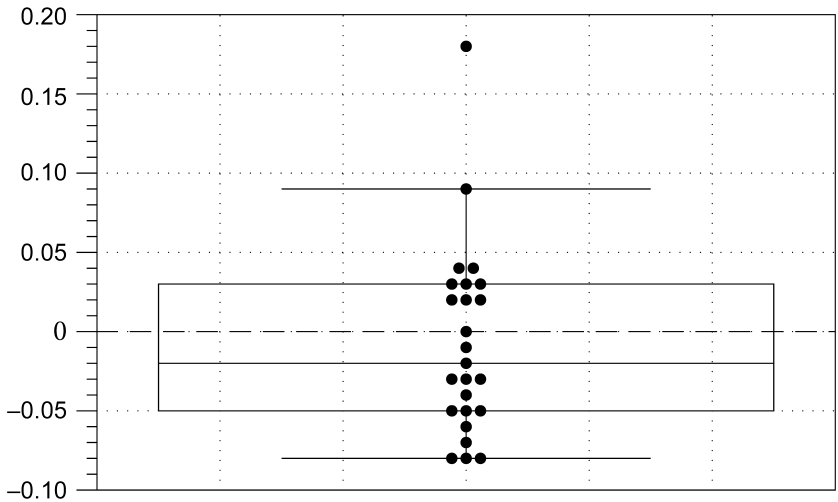


TABLE 8.4 T-Test of State Affinity in Year Prior to Conflict

Number of values	25
Mean	0.1804
Std. Deviation	0.5016
Std. Error	0.1003
Lower 95% CI of mean	−0.02664
Upper 95% CI of mean	0.3874
One sample t test	
Theoretical mean	0
Actual mean	0.1804
Discrepancy	−0.1804
95% CI of discrepancy	−0.02665 to 0.3875
t, df	t=1.798 df=24
P value (two tailed)	0.0847
Significant (alpha=0.05)?	No

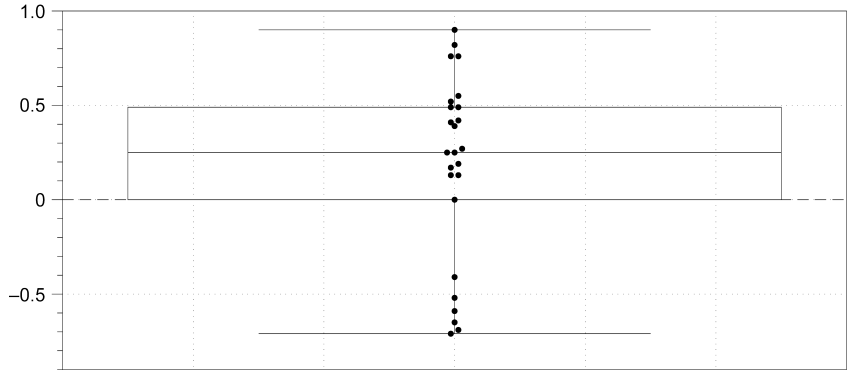
because there are a limited number of cases, it is impossible to draw statistical significance from these results. If, however, the results are examined using the a = .1 threshold, it is possible to indicate that cyber attacks are more likely between states with positive affinity scores than between states with negative affinity scores. Anecdotally it is possible based on the data to infer that states with close policy affinity scores are more likely to engage in cyber hostilities against one another than states with negative affinity scores.

If we take a step back and look at the six of twenty-five cases with negative affinity scores, several striking characteristics stand out. First, all of the cases in which there was a negative affinity score included either the United States or Israel. Second, in five of the six instances with a negative affinity score, the attacking party or parties had a significant power advantage. Only one instance, a CE attack by China against the United States, stands out.

These results indicate that at a = .1 there is a statistically significant relationship between positive state affinity and likelihood of conflict. Although Bueno de Mesquita indicates that this relationship is likely due to anticipated changes in policies or behavior at a future point in time, the results are therefore inconclusive and do not support such a conclusion with the limited data available.[30]

The tests of *Propositions 3 and 4* are broken into two separate tests because the propositions intrinsically encompass two different hypotheses. The first hypothesis is that states are more likely to attack states when the expectation is that there is deterioration in the relationship over time. The second hypothesis is that states are more likely to attack when states are more closely aligned along the policy spectrum. Neither of these hypotheses is proved significant at the a = .05 threshold.

FIGURE 8.4 Distribution of State Affinities in Year Prior to Hostilities



DATA IN CONTEXT

The data presented in this analysis span twenty-three unique incidents with twenty-five cases. What is evident from the data is theoretical connection between anonymity for instigators of cyber incidents and rational behavior. If anonymity is removed from the decision-making process, then attacks within the cyber domain are irrational. In the present context and based on everything known about interactions within the cyber domain, anonymity is a defining concept of cyber conflict. Beyond the necessary inclusion of anonymity for decisions to be rational, the data indicate a propensity—although not statistically significant—for conflict between states with positive policy affinity scores and indicate no definable relationship in changes in policies over the established one-year time frame to the instigation of conflict.

It is not unsurprising that the majority of incidents occur between states with relatively positive affinity scores. To be worthy of an attack a target must possess a level of development that exceeds a minimum threshold in most instances. This is particularly true when considering the impact or the potential take from midrange attacks. Because most of the targets exist at the higher end of the developmental spectrum of states, it is intuitive to assume that is where the attacks would likely occur. When attacks extend beyond simple operations into more complex incidents such as Stuxnet, they are focused not on a broad take of information or a systemic change in relative capabilities; rather, the focus becomes a single system of value. It doesn't do much good for a developed country to attempt cyber attacks against an undeveloped country unless that country has definable targets. However, because developed countries share many of the same interests, it is not unreasonable to assume that targets within these countries hold special value to their developed nation counterparts. This indicates

that as states diverge on policy issues, even if they are still positive in policy affinity, it makes sense to seek out why the divergence is occurring or attempt to shift this divergence in another direction. This then leads to cyber conflict. To more closely examine this aspect of cyber conflict far more data are necessary than are currently available.

Availability of data is one of several major areas of room for improvement within this work. The argument in aggregate contains several areas in need of improvement. These areas are less methodological in nature than they are data driven. First, there is no exact measure of anonymity. The measure at present is a rough estimation predicated on type of incident. As was indicated in chapter 5, it would be best to use a statistical function such as a hazard function populated in with intelligence. Enhanced measures of anonymity would dramatically increase the accuracy of the model.

Second, there are a limited number of cases included within this study. To fully parse out each of the propositions would require more cases. Many of these cases are available, but they are currently publically unavailable for various reasons and are therefore unavailable to facilitate a more dynamic and robust analysis.

Third, the power score in this model is kept artificially static over time. The static nature of the power score is due to insufficient data availability across time even within the limited sample of nations present within this study. Any study attempting to expand the data outward either longitudinally or latitudinally will quickly run into data collection problems on even the most basic indicators of digital power. This data issue is improving as organizations such as the International Telecom Union continue to compile robust data.

Fourth, it is possible that the use of United Nations voting affinity scores artificially places nations in closer policy proximity than other measures of state policies within the international context. Similarly, the U.N. affinity scores only constitute a small sampling of interstate interactions and therefore do not serve as an all-inclusive measure of relative state policy positions.

Lastly, because there are no evident cases in which a state initiated conflict under conditions of political utility, and because there is no accurate measure of the success of different types of attacks in the form of peace treaties or other documents delineating the victor to a particular conflict, data analysis is limited to disaggregated hypothesis testing. This is a departure from Bueno de Mesquita's use of Yule's Q tests as a means of identifying a proportional reduction in error. The study of conflict within the cyber domain is a new and evolving field of research. While there are millennia of data on conventional conflict, cyber conflict has only been around for approximately thirty years in its present form. Over time, as the number of cases increases, the ability to employ more robust statistical methods will enhance the ability to study this new domain.

CHAPTER 9

Cognitive Processes and Decision-Making in Cyberspace

PEOPLE ARE COMPLEX. Irrespective of how much effort we put into establishing parsimonious models of human behavior, the fact remains that human beings are inherently irrational. To this point this work has established, using a parsimonious framework based on expected utility, the foundations for why states engage in cyber attacks. The theoretical framework established fits well within the paradigms of international relations and explains behavior in a pleasing fashion to build a testable set of conditions. Yet the argument presented over the course of this book for the rational decisions of states in cyberspace would be remiss if it did not account for the inherent cognitive limitations of a unitary decision-maker. Although a unitary decision-maker is assumed to be rational, it is also important to consider that this decision-maker is human and therefore vulnerable to cognitive biases. Below are several examples of cognitive biases that might influence the decision-maker to engage in a cyber attack under circumstances with a negative expected utility.

It is estimated that there are in the range of fifty-eight different cognitive biases that influence human cognition when making decisions. To examine all fifty-eight biases in relation to cyber decisions would constitute a book unto itself; therefore, to illustrate how irrational behavior might influence a decision-making process, the analysis here examines only a very small subset of cognitive biases that have been previously examined within the context of economics and international relations and found to have a significant effect. The intent is not to be all-inclusive of the cognitive aspects of choice associated with state decisions to engage in offensive cyber operations or to go very deeply into inner workings of these cognitive biases, but rather to provide a foundation for falsifying the rational argument advanced in this book. Through the process of falsification this chapter seeks to establish that the rational choice model, while imperfect, offers a parsimonious and accurate way to conceptualize state decisions in cyberspace.

PROSPECT THEORY

The biggest challenger to expected utility theory over the past several decades comes from Daniel Kahneman and Amos Tversky through prospect theory.[1]

Prospect theory hones its critique of expected utility on the non-utility maximizing behavior of individuals under conditions of risk. Tversky and Kahneman illustrate that individuals violate the fundamental tenets of expected utility through a cognitive bias in how they process probabilities for gain and loss. Their work illustrates that individuals, under conditions of risk and within certain heuristics, privilege the potential values of loss and gain, rather than final outcome values. By privileging potential values of loss and gain, individuals are discounting risk. The privileging of expected values of risk and loss rather than actual final outcomes associated with cyber conflict manipulates the probability functions associated with anonymity and leads individuals to engage in riskier actions than would rationally be expected under certain circumstances, while avoiding less risky actions in situations that expected utility modeling would deem rational.

Why does bias matter for actors in cyberspace? Jeffrey Berejikian illustrates that this changes the way in which states deter actions of other states and thereby creates systemic problems with the concept of power measures based on capacity and credibility.[2] He finds that deterrence is not consistent and changes as the value associated with loss and gain changes. This manipulates the transitive preference ordering of a rational choice. In particular the effect of deterrence is influenced as the actors' valuation for given action changes based on relative expected losses or gains. At its most basic it is conceivable, under the conditions demonstrated by prospect theory, that actors might engage in cyber attacks absent positive expected utility or abstain from attacks in instances in which utility is positive.

Robert Jervis also takes on prospect theory and identifies additional implications for international relations that carry over to the expected utility of cyber conflict.[3] Jervis indicates that states averse to risk will be more cautious when deciding to engage in military actions to influence the bargaining range. This aversion to risk and its effect on the probability function associated with anonymity makes states less likely to engage in offensive cyber operations than they might otherwise be. However, once an offensive operation commences, Jervis's argument suggests that a state might devote substantial resources to cover up or hide even trivial transgressions.[4] The bias introduced alters the risk/reward calculus of engaging in continued operations and might lead a state to engage in irrational behavior. The implications of a cover-up operation could turn what was originally a small OCO into a large OCO and thereby alter the aggregate utility calculus for a single operation by essentially making a single operation with a unique expected utility into a compound function based on the interrelation of two operations. This would violate the fundamental assumption of indpendence for rational decisions and invalidate the model.

In brief, this illustrates the many implications of prospect theory that can affect everything from the bargaining range between states and deterrence to

general war/peace decision-making. Further extended study on state actions based on prospect theory might further elucidate behavioral patterns and facilitate the development of a cognitive model for decisions to engage in offensive cyber operations. Although the effect of prospect theory in relation to the vaulation of loss and gain was not demonstrated in the expected utility model for international cyber conflict, it has the potential to undermine the reliability of the model. The biases demonstrated by prospect theory make it difficult to consider expected utility theory as the only means by which to explain state behavior in cyberspace. It should be noted that although this poses theoretical challenges to the model developed in previous chapters, it does not obviate its explanatory power but rather conditions it.

The conditioning of the expected utility theory of cyber conflict based on prospect theory could be helpful in instances in which the relative values associated with loss and gain might significantly bias a decision-maker. Although prospect theory is extremely powerful and has been demonstrated in studies at the individual level, it has also been found to contain problems at the aggregate level. Furthermore, because the rational model presented in this book is dynamic and informed by significant amounts of data on both the capabilities and vulnerabilities of states and probability of maintaining anonymity during a given operation as well as concepts of risk and uncertainty, it is possible that many of the biases associated with prospect theory might be mitigated, at least in part. Yet, as the uncertainty and risk associated with a given cyber attack increases, risk aversion is likely to play an important role and should therefore not be entirely discounted.

CONSTRUAL LEVEL THEORY

Construal level theory (CLT) is another set of cognitive theories that challenge the construction of expected utility models. First examined in the context of international relations by Ronald R. Krebs and Aaron Rapport, construal level theory indicates that individuals perceive events in terms of differing types of psychological distances.[5] These distances can include temporal, social, and spatial distance. It is understandable why decisions regarding cyber operations would fall victim to issues associated with psychological distance biases. Expected utility theory at the state level is a high-level conceptualization, and many expressions of expected utility theory assume the benefits of actions associated with expected utility are consistently (monotonically) discounted over time in what has been referred to as a "discounted utility."[6] In contrast, the utility argument present in this book established a nonmonotonic decline in expected utility predicated on using a hazard function to determine the probability for the loss of anonymity over the course of an offensive cyber operation. Although

the model presented in this book does not assume a monotonic loss of utility, it fails to consider the application of psychological biases that separate different actors' concepts of value based on psychological distances across time, space, and social constructs.

Psychological distance is applicable because decisions on offensive cyber operations occur within temporal constraints under conditions of anonymity, social constraints of interpretation and target psychological impact, and spatial constraints of abstract systems in distant networks. CLT has primarily been examined in experimental psychology yet carries over with broad application to international relations decision-making. Nira Liberman and Yaacov Trope first published an article on CLT in 1998, which garnered significant interest and has since served as a foundation for discussion and experimentation.[7] Liberman and Trope argue that perception is egocentric and based on the person's present position temporally, spatially, and socially relative to a future event, distant place, or different social environment.[8] As an event becomes increasingly distal from the point of origin, the more abstract the associated attributes of that event become in the mind of the decision-maker. Temporal abstraction is necessary in cyberspace as in conventional attacks because a decision-maker assumes a change in status and subsequently the ability to affect a target over time. The effect of pressing the button on a computer to instigate a cyber attack is very different from the effect an OCO will have on a system down range. Because individuals abstract outward from their present position, psychological distance biases a decision-maker's decisions on action or inaction.

Pyschological distance has significant ramifications for both offensive and defensive cyber operations. For example, when in a defensive position, it could be assumed that a behavior in cyberspace is purely espionage related and therefore does not warrant a strong response action. Because the event is proximate, the decision-maker concretely interprets the attack as espionage but fails to see the broader strategic implications of an attack and therefore does not implement precautions against abstract threats associated with a given incident. It is possible that the Operation Cleaver attacks conducted by Iranian hackers, examined in chapter 3, were solely for espionage purposes. The attacks all appeared to be of moderate complexity but did not directly modify or damage critical infrastructure. However, as noted by Cylance, this assumption would likely be a mistake as the abstract ramifications of the attacks might have significant consequences at a future date.[9]

Spatial distance also presents significant problems for decision-makers. Marlone D. Henderson et al. find that when individuals think about objects as spatially distant, they construe the object more abstractly.[10] Within this context the Stuxnet worm was designed to attack the network associated with highly enriched uranium (HEU) production at Natanz, or even more abstractly Iranian

nuclear production facilities, rather than specific types and configurations of Siemens centrifuges and the Windows computers used to manage operations. Although some abstraction is necessary for decision-makers, too much can obfuscate potential externalities associated with attacking systems or can induce decision-makers to opt for inappropriate attacks because the distal target looks "easy" to attack when considered abstractly. Abstraction can also hinder debates on whether to engage in a particular operation, as it can cause two individuals to discuss the same system in different ways and can thereby result in confusion, as has been evidenced in academic debates on the actual target(s) associated with the Stuxnet attack.[11]

Spatial abstractions relating to offensive cyber operations is a larger problem than it might at first appear, due to the inability of most nontechnical decision-makers to fully understand the systems being targeted. Because they are abstracting the concepts of cyber operations away from specific types of attacks against targets within often complex network environments, there is a possibility of becoming overly optimistic about the probability of achieving utility. It is not uncommon for technically inclined operators to hear wild requests in terms of operations against spatially or temporally distant targets from nontechnical individuals. Similarly it is not uncommon to have students ask their professor, "Why can't we just use cyber operations" to "take out the power grid," "take down their airplanes," or any number of similar statements.

Abstraction in spatial terms can be helpful in many operational environments. Abstracting outward facilitates a commander's decision to maneuver units on a battlefield based on assumed capabilities. One of the reasons all soldiers must pass basic fitness tests or qualifications is that it assists a commander in making abstract decisions rather than always needing to identify individual soldiers fit enough or skilled enough for each particular operation. Yet when the abstraction becomes too great, the assumed ability to accomplish a mission falls victim to error, and the ability to make a rational decision becomes unlikely.

Lastly, construal level theory also posits issues associated with social distance. Gabriela M. Jiga-Boy, Anna E. Clarke, and Gun R. Semin posit that social distance can affect the interpretation of a message being sent and the subsequent relationship of the sender and receiver.[12] The authors of the study indicate that understandings of social abstraction can influence the understandings in interpersonal interactions. Although their study specifically focused on individual-level analysis of interpersonal communications by shifting the focus away from individuals to state-level interactions, it is possible to conceive of the problems raised by social distance.

Social distance plays a significant role in interstate communications and perceptions. For example, many commentators on Chinese development in cyberspace tend to focus on the concrete actions of the People's Liberation Army

(PLA) from an American- or Western-centric focus. The social context of PLA cyber operations is sometimes construed proximately as hostile and similar to acts of cyber warfare by select scholars and experts.[13] Yet China's behavior is regarded as primarily defensive in nature by others.[14] Because offensive cyber operations as a form of covert action are designed to influence and accrue positive utility to the attacker, an accurate understanding of the adversary is necessary. If an attack is unable to shift the behavior of the target or to provide leverage by which to manipulate the bargaining range between two states, then it is possible the social distance between the two parties distorted the decision set associated with an operation or altered an operation such that it was unable to achieve the desired goal.

Using the U.S.-China relationship as an example of social distance, it is reasonable to discern social distance between the two states' perceptions of cyber espionage (cyber intelligence). Here the discussion becomes one of fundamental disconnects between the shared knowledge frameworks of the two cultures. Espionage for corporate gain in the United States is seen as unfairly privileging businesses in a free market system. Robert Gates, the former director of the Central Intelligence Agency, summed up the argument against corporate espionage best in a testimony before the congressional intelligence committees in April 1992: "[U.S. intelligence] does not, should not, and will not engage in industrial espionage. . . . Plainly put, it is the role of U.S. business to size up their foreign competitors' trade secrets, marketing strategies, and bid proposals. Some years ago, one of our clandestine service officers said to me: 'You know, I'm prepared to give my life for my country, but not for a company.' That case officer was absolutely right."[15]

The Chinese perspective and moral, cultural, and ethical framework differs from U.S considerations. The United States regularly accuses China of engaging in espionage for corporate gain that it sees as unfair and unethical practice. However, because China is a communist, authoritarian system, the Chinese view the gain as national security in context and view espionage as attempting to level the playing field in which they perceive themselves as the weaker state.[16] Whereas signals to induce or compel a state to cease espionage activities for corporate gain might work in a Western context due to social proximity, the same signals might be taken as overtly hostile when viewed through a distant social construct. Indictments in 2014 of Chinese nationals suspected of engaging in cyber espionage establish concrete rather than abstract signals to indicate extreme displeasure by the United States.[17] By reframing the issue within a mutually understood framework, the social distance is reduced.

Social distance does not imply that it is impossible to provide accurate signals. Instead, social distance implies that developing communications or signaling under the issues identified by CLT requires understanding the level of

abstraction relevant to a given situation. Thus, broad abstractions such as corporate espionage might not be based on the same cognitive foundation and therefore necessitate a more concrete reference point upon which a shared understanding can be forged.

A DDoS attack against a state by hacktavists will likely be interpreted by a state as criminal behavior, whereas the same attack by a state against another state could be consitutive of an act of aggression or a prelude to other forms of conflict, as in the case of the Russia-Georgia war of 2008. Understanding the shared social environment removes misinterpretations due to social distance and facilitates more effective operations. The expected utility model for cyber conflict does not include mechanisms for understanding social distance and instead assumes social distances into a mathematical function. Failing to comprehend the social distance between the sender and receiver of a signal might damage the ability of a given cyber operation to effect substantive policy changes. Therefore, the same action conducted by two separate actors might result in two different utility caculi: one that generates meaningful policy change and one that doesn't. This illustrates a flaw in expected utility modeling by highlighting that there are more attributes associated with decisions than a mathematical calculus based on predefined variables.

ACCURATE AND PREDICTABLE

When deciding to employ cyber weapon systems against state targets, cognitive understanding of decision-makers and their targets helps condition a decision to achieve a maximum effect. Cognitive models suffer in their extensibility (or lack thereof) and therefore are of limited use when developing diverse models of phenonena. Although repeated behavioral traits and consistencies across certain cognitive biases have been identified, others are inconsistent across individuals or vary within individuals. Cognitive biases that vary intrapersonally as well as interpersonally make it difficult to develop a parsimonious model to explain how the world works. Cognitive approaches illustrate the failings of utility-maximizing models, yet they do not necessarily offer a one-stop shop for better alternatives; rather, they present a mix-and-match circumstance of dependent conditions that decision-makers need to understand. The inconsistent application of many cognitive models makes predicting state behavior difficult and reduces aggregate explanatory power. In contrast, the expected utility model, while subject to the deficiencies of cognitive models, can still present a broad model with extensive explanatory power. Morever, the ability to engage in consistent repeat verification and falsification of the model provides a heuristic upon which to build more explicit decision-making models for state actions in cyberspace.

CHAPTER 10

Finding Meaning in the Expected Utility of International Cyber Conflict

> Cry "Havoc!" and let slip the dogs of war, that this foul deed shall smell above the earth, with carrion men, groaning for burial.
>
> Mark Antony in Shakespeare's *The Tragedy of Julius Caesar*

CYBERSPACE, as the previous chapters have demonstrated, constitutes a unique and important domain affecting various aspects of national security. The importance of cyberspace to modern society is undeniable. Comprehending state decisions in a domain that has become such a ubiquitous feature of daily life for billions of people around the world is a fundamental first step toward integrating this domain into the broader field of security studies and international relations. By focusing on a rational choice approach to the decision-making process and honing the decision process using expected utility, this book illustrates a novel approach to understanding how states interact within cyberspace. This final chapter examines the implications of the expected utility theory of international cyber conflict and examines how these implications influence a wide spectrum of issues related to international relations applicable to policy-makers.

THE BOTTOM LINE

States are mostly rational actors in cyberspace when anonymity is taken into consideration. Despite attempts over the years to disprove or diminish the usefulness of rational choice, the evidence presented in chapter 8 and the combined weight of the argument developed over all of the chapters should provide some comfort to decision-makers that state decisions to engage in offensive cyber operations are not ad hoc, but deliberate and rational. This does not preclude the possibility for irrational state actions in cyberspace; however, it does establish that much of the literature on international relations is still largely relevant.

Why is this important? As discussed in earlier chapters, there is a tendency to exaggerate the threat of cyberspace and to compound its possible effects on international order by stating that the domain is categorically unique and the

rules of international politics do not apply. Instead, cyberspace should be considered a domain of state interactions with identifiable behavioral patterns that can be examined within existing theories. While the specific attributes of the actions themselves might be new, the ability to comprehend the decision processes and the resultant desire to achieve effects are not. Cyberspace is not an inherently irrational domain, nor is state behavior in it inexplicable.

Operations in cyberspace are not dissimilar from the beginning of any new arms race. New technologies have been created that are complex and growing ever more so as computing power advances and human interactions within the domain increase and gain importance. Cyber weapons have destructive power; yet the extent of that power is uncertain and likely to substantively evolve in the coming decades. It took hundreds of years for guns to develop to the point where it became irrational to march soldiers in lines at one another. When the frequency and accuracy of fire made the losses associated with certain strategies and tactics too costly, new strategies and tactics were developed. Not only is cyberspace still developing technically, but it is expanding geographically as connected computing devices proliferate, and its relative value to humanity is expanding as more and more individuals leverage cyberspace in daily interactions. Decision-makers should expect cyberspace to become increasingly difficult to manage as it expands. Yet despite its increased complexity and importance, the ability to predict state behavior remains largely unchanged. Just as guns did not change the desire of states to engage in wars, neither will cyberspace. The strategies and tactics used in cyberspace will change as cyber weapons improve in effect and lethality in much the same way they did when guns changed from muzzle-loading rifles to automatic cartridge or belt-fed weapons.

THE DECISION TO ATTACK: DECISION-MAKING FOR OFFENSIVE CYBERSPACE OPERATIONS

States engage in offensive cyber operations when they have positive expected utility. Positive expected utility in cyberspace is largely predicated on an assumption of anonymity that does not monotonically decline from the point of attack initiation to attack completion but is instead a decline conditioned on the scale and complexity of an attack. Without such a measure the conduct of offensive cyber operations in most instances would be irrational. Even the inclusion of modest measures of anonymity enables the generation of positive expected utility.

Anonymity opens Pandora's box for cyber conflict on the state level. Without constraints imposed by potential losses, anonymity makes rational actors of almost all states in cyberspace. Anonymity makes it possible for states at a traditional power disadvantage to engage in hostile acts against more powerful states.

This leads directly to the quote at the beginning of this chapter from Shakespeare's *Tragedy of Julius Caesar*.[1] Because anonymity reduces the ability to deter by means of power or skill in most instances, the proverbial dogs of war are unleashed. If the only constraints on offensive actions are moral and ethical, why not engage in bad behavior? Bad behavior in cyberspace is rational because there are few consequences for actions conducted in the domain. Russia did not suffer any meaningful consequences for sponsored or condoned cyber operations against Estonia and Georgia, nor did the United States and Israel suffer for the Olympic Games program or the disabling of Syrian air defenses. None of the states that engaged in offensive cyber operations across the sample presented in this book had any reasonable expectation of loss associated with their actions. The absence of reasonable expectations of loss should not imply that loss is not possible, but rather that the possibility is so small that it does not constrain behavior.

Cyber conflict on a midrange scale, where anonymity is strongest, is likely to continue to grow until states are able to place constraints on actions. Because the probability of maintaining anonymity decreases with the complexity and size of attacks, the likelihood of major state-on-state cyber conflict should be low. However, as noted in chapter 2, midrange cyber conflict results in a death by a thousand cuts. Because much of the technology and many of the strategic plans associated with national security are stored at these lower levels, this death by a thousand cuts decreases the relative conventional power of states.

The data illustrate that although China is at a relative power disadvantage and would likely not engage at present in conventional attacks against many states in the international system, it is willing to engage in offensive cyber operations and cyber exploitation because it can do so with impunity. China's cyber activities have arguably increased its conventional power, relative to that of its potential adversaries within the international system. Although there is insufficient evidence to make broad generalizations, the trend established by the Chinese is likely not isolated. Anonymity favors the attacker in nearly all situations within the cyber domain. Despite assertions by Jon R. Lindsay in an article on the limits of cyber warfare that there is little evidence to suggest an offensive advantage in cyberspace, the overwhelming evidence at both the state and substate level would contradict this.[2] Due to anonymity, the instigator of a conflict has an advantage in choosing where and when to attack. Because of an offensive advantage it is likely that cyberspace will remain an increasingly hostile domain until such time as there are effective methods for reducing the probability for maintaining anonymity when engaging in offensive cyber operations. This should not be taken to mean that there will be a cyber Pearl Harbor or other extravagant attacks. Instead the cyber domain is likely to see a steady tempo of hostilities with occasional spikes in scale and complexity as capabilities are developed and utilized.

Hostilities aside, a state's development of all aspects of cyber power will affect its power relative to that of other states within the international system far more acutely within the cyber domain than in conventional domains. Because cyber power is characteristically different than conventional power, it is not sufficient to simply build cyber weapons; instead, it is necessary to educate engineers, to build stable infrastructure, and to establish laws and regulations that can adapt to a rapidly changing environment. It is also important to educate the population of a country. As a population is educated to recognize cyber threats, there should be a corresponding reduction in the aggregate level of national vulnerability. Power scores indicate that it requires a balance between multiple aspects of a nation's development to achieve cyber power. As a state becomes increasingly dependent on the cyber domain, the importance of improving the qualities associated with cyber power increases. Although cyber power does not necessarily mitigate the effects of anonymity, it helps to influence the decisions of states. A state with a higher power score is more likely to undertake more complex actions, even if it is unable to maintain indefinite anonymity. Combined power and anonymity are important variables informing the decision-making process associated with state construction of utility for offensive cyber operations.

Expected utility as a result of covert action broadly, and more specifically as a result of offensive cyber operations, was developed in detail in chapter 3. Covert actions of any type should be considered instruments of the state designed to achieve political utility. The case that political utility can be achieved through covert acts facilitates an understanding of not only why states engage in covert action, but also why they engage in covert actions in the form of offensive cyber operations. If, as was argued, covert acts work within the bargaining range between overt conflict and overt diplomacy, this middle and underexplored territory broadens the understanding of conflict processes.

Political utility achieved through covert offensive cyber operations shifts an opponent's policies to a more favorable position or slows policy divergence. Not every OCO is able to achieve positive utility, just as not every military operation or diplomatic negotiation succeeds. Failures to achieve the desired benefits of a given action abound across the spectrum of conflict and diplomacy. Covert actions, especially OCOs, are no different. The motivation for a covert OCO is the possible realization of political benefit. If this realization of political benefit occurs through anonymous actions in cyber or through kinetic weapons that go boom, the objective is still the same.

The study of utility derived through covert means and the motivation behind those means lags behind other areas of international relations largely because data are not readily available, particularly for recent events. A lack of data leaves the study of covert action in cyberspace, in particular, understud-

ied, ignored, or misunderstood. Although this book primarily examines covert cyber operations, the data on broader covert acts are difficult at best to come by. This book attempts to use similar cases to provide a rigorous study of the potential for political gain through operations conducted anonymously. The data are limited and although there are aspects that are statistically significant, future data will enhance the discussion and refine the modeling techniques presented.

FAILINGS AND AREAS FOR IMPROVEMENT

Like any new vein of research, there are likely to be areas in need of improvement. The argument presented over the course of this book needs to improve in three primary categories: data, methodology, and theory. Improvement across these categories will increase the rigor and explanatory power of the work.

Data are a social scientist's best friend, but also a social scientist's worst enemy. When studying any form of covert action, cyber included, data on a large scale are often missing. If states acknowledge a role in either the defense or instigation of a cyber attack, they release information about their capabilities and defeat much of the advantage associated with OCOs. Therefore within the study of cyberspace, the first major obstacle is data on attacks themselves. Often this lack of data is due to an unwillingness of a state to admit it has fallen victim to an attack. However, it is equally as likely the state is aware it has fallen victim to an attack but is unaware of the source of that attack.

Data problems do not end with the inability to accurately identify attacks and participants within the cyber domain. To fully develop utility it is necessary to construct an accurate measure of cyber power. Data availability on this measure spans legal and regulatory, economic and social, infrastructure, industrial, military, and demonstrated capability measures. Longitudinal availability of data across these measures is severely limited due in many respects to the newness of the field as well as the rapid expansion of the domain itself. Collection on even the most basic indicators related to the cyber domain is new and primarily limited to developed countries. This makes a thorough analysis over time extremely arduous at present.

Data limitations create methodological problems preventing more robust statistical analyses. To test the argument for expected utility associated with decisions to engage in OCOs, *t*-tests were used to test propositions. It is possible that more data across a larger sample would provide more robust results or indicate results that diverge from the hypothesized relationships. Likewise, because data on the probability of maintaining anonymity were assumed based on the classification of attacks rather than on more specific information analyzed in a hazard model, it is possible the results are skewed to favor anonymity in inci-

dents where anonymity is less important. Continued collection of data will only increase the accuracy of the model.

Beyond the methodological and data issues, this work contains some fundamental theoretical questions that need to be briefly addressed. Any study on decision-making should consider the theoretical foundations of a decision. In this book rational choice was used as that theoretical foundation. It is important to concede that there are numerous cognitive studies indicating human beings are, in fact, not rational arbiters, the most famous of which are Kahneman and Tversky's study on prospect theory and Liberman and Trope's construal-level theory examined in chapter 9.[3] Does a lack of rationality diminish the results of this analysis? Based on the assumptions presented and the results of the analysis, there is a mathematical logic behind state instigation of cyber conflict.

Although the theoretical foundation of this logic is based on rational choice, and rational choice has been shown to have inconsistencies, the results indicate a significant relationship between positive utility and instigation of conflict. Within the Center for Strategic and International Studies report on significant cyber incidents in which two states were listed as parties to a cyber conflict in either a defined or undefined fashion, there was not a single incident in which a state instigated an OCO with a negative utility when taking into consideration the assumption of anonymity.

The results indicate that even though there are theoretical failings within rational choice theory, the theory accurately predicts state interaction. Echoing Milton Friedman's thoughts, the theory advances that an economic theory should be judged not by its realism but rather by its ability to predict phenomena.[4] Therefore, the simplicity offered by the rational choice–expected utility approach to decisions within the cyber domain offers a parsimonious and predictable conceptualization of the world.

Despite this dependence on rational choice, it would be useful for future analyses to examine the effect of cognitive behaviors such as prospect theory and construal-level theory in more detail. These other veins of research will become increasingly helpful in understanding the decision-making processes involved in conflict within the cyber domain as data availability increases. Until data availability improves, studying these cognitive theories in the cyber domain is likely to be difficult, if not impossible.

THE IMPLICATIONS OF THE EXPECTED UTILITY THEORY OF INTERNATIONAL CYBER CONFLICT

Returning full circle to the research question, this book investigates how unitary state actors rationally decide to employ offensive cyber operations for political gain. It contextualizes broader cyber decision-making processes into a system-

atic expected utility–rational choice approach to provide a mathematical understanding behind the use of cyber weapons at the state level. Understanding the rational choice decision-making process states employ in deciding to use cyber tactics formed a contextual foundation upon which to build rational offensive and defensive strategies for cyberspace. This book provides the evidence and theoretical foundation for an expected utility–rational-choice decision-making model for the instigation of cyber attacks. To investigate this it was necessary to construct a new decision-making model with its foundations rooted in Bueno de Mesquita's expected utility theory of international conflict.[5]

The major lessons learned suggest there are three concepts that have been developed with regard to the cyber domain that are either unique to the domain or necessary for actions to take place within it. The concepts of power, anonymity, and political utility for covert acts are pivotal to understanding state-on-state interactions within cyberspace. Just as there are indicators of international political economy, conventional conflict, and every other subject area within the subfield of international relations, there are qualities within the cyber domain that must be included for a study of decisions within the cyber domain to be successful. These lessons open up a realm of discussion not only on topics pertaining to the domain itself but also on other types of covert action more broadly. The subfield of international relations has long ignored covert action by theoretically and methodologically pushing it aside. This study attempts to bring back into the fold this often-overlooked area of action and to steal a distinctly political act partially away from intelligence historians and reestablish it within international relations.

The positive utility of OCOs under anonymity is clear and unambiguous. It is possible to generate political utility within the cyber domain through hostile acts. Asymmetry between states matters in the context of anonymity, yet it also shows that brute power can still overwhelm and that attacks can originate from anywhere if the conditions are favorable. This book tests this claim and finds that in many cases a less powerful state can and does initiate hostile acts against a more powerful opponent not necessarily because of a relationship in terms of power but because, like the criminal who can rob a bank without fear of prosecution, there is little stopping it. As the scale and complexity of an attack increases, the probability of maintaining anonymity decreases and therefore the probability that a small state or that a state of any size will engage in a massively damaging cyber attack will still necessarily involve traditional concepts of power and deterrence.

When anonymity was excluded, the conventional thought process on power prevailing still held in all instances with regard to utility. The evidence suggests the largest and most complex types of attacks are still relatively limited to large powerful states, and that those attacks offering higher probabilities of anonymity

are still viable to middle range actors. Yet the realization that asymmetry won't result in small states rationally engaging in large-scale, complex OCOs should not be wholly welcoming news. Mid-level attacks against critical infrastructure, banking, social/political, and environmental elements of national security threaten to undermine national security and confidence.

The power scores developed for this argument indicate a complex understanding of state capacity to engage in offensive and defensive actions in cyberspace. A complex and nuanced understanding of power might surprise many defense theorists who assume that military budgets alone make the biggest difference in all-around national security. Instead, what the power scores indicate, in both their theoretical development and their combination into an overall measure of state power, is a complex relationship within cyberspace that relies on broad and concerted efforts across government and civil society. As countries become more dependent on the domain, it becomes increasingly necessary to ensure the pillars of national security through the education of engineers, the writing of logical rules and regulations, and a level of national vigilance across the civilian government, military, corporate realm, and citizenry.

The construction of power in cyberspace presented here provides a broad estimation of national digital vulnerability; this number could be relatively minimized if all aspects of society were to focus on improving their digital hygiene. Improved digital hygiene will not eliminate all threats in cyberspace, but just as vaccinations haven't eradicated all diseases, they have significantly reduced the prevalence and severity of outbreaks. Cyberspace is a man-made domain, and the best way to improve national security in this domain is to begin developing herd immunity. Herd immunity in cyberspace will not mitigate all threat vectors or eliminate all risk. Yet it is likely to begin a process of reducing the aggregate attack surface from a seemingly infinite number of vectors to a more manageable set. One of the reasons for the scale of asymmetry in cyberspace beyond anonymity is the asymmetric attack surfaces of different nations.

Earlier it was argued that North Korea has a relative advantage in terms of target selection compared to the United States within the cyber domain. The FBI in December 2014 provided significant evidence tying North Korea to a significant cyber attack against Sony Pictures Entertainment (SPE).[6] Sony and multiple movie distributors then declined to distribute and show a controversial satire in which North Korea's leader Kim Jong-un was assassinated.[7] The exploitation of Sony did not constitute an attack against national security in the traditional sense. Sony is not tied to critical infrastructure, and the attack has a limited economic impact on the American economy. Although the FBI directly tied the attack back to North Korea and the United States threatened some form of response, individuals claiming a cyber response is warranted largely missed the asymmetric relationship of the targets. North Korea, with minor plausible

deniability, was able to achieve a political goal of preventing the release of a movie in the United States. Meanwhile the United States and its allies have only limited avenues for response. It should also be noted that while the attack was believed to be related to North Korea from its start, the anonymity of the operation through the completion of its objective to steal and release large volumes of data and pressure the company and its distributors not to release the film was successful. All told, the relative power combined with even limited anonymity made it possible for North Korea to achieve political utility.

The Sony hack should serve not as a rallying cry to weaponize cyberspace more than it already is or to provide national security support to corporations not directly tied to national security interests, but rather as a confirmation that the fundamental attributes of the expected utility model for cyberspace mean that a state can successfully alter the behavior of adversaries if it can maintain even modest amounts of anonymity so long as its attack surface is small. It also illustrates that targets not directly related to national security can impact a nation's psyche. The Sony attack should serve instead as a call for local, state, and federal lawmakers to begin providing incentives for companies to enhance their own security practices and protection of information as well as corresponding disincentives when companies fail to take even basic cyber security precautions. The United States is rapidly moving to incentivize cyber security across critical infrastructure under Executive Order 13636, yet the economy as a whole is so heavily reliant on cyberspace it is likely that to facilitate a culture focused on a secure and free cyberspace, broader national initiatives will need to be developed.

The development of cyber security at the national civilian, governmental, military, and critical infrastructure levels has advanced enormously over the previous five years since work on this book began. Fleet Cyber Command of the U.S. Tenth Navy began in 2010, along with its counterparts including the Second Army–U.S. Army Cyber Command in 2010, and the Twenty-Fourth Air Force–Air Forces Cyber in 2009 have all been stood up, or created. In September 2014 the U.S. Army officially created a new career track, a cyber branch, specifically devoted to developing training and equipping cyber warriors. Beyond the service-level changes, the service academies and ROTC are in the process of developing cyber programs to provide skilled officers able to protect the United States against a variety of threats emanating from the cyber domain within the next few years and decades. Within the civilian government, organizations such as the Federal Bureau of Investigation, the Department of Homeland Security, the Department of the Treasury, and many others have been working to develop specialized cyber units to enhance national security in cyberspace. The task is enormous. In the federal government alone there are millions of computing devices spanning around the globe and into space. Yet progress is being made.

The debate over whether cyberspace is important to national security has seemingly been solved everywhere except in academic debates. Federal, state, local, corporate, and private allocations of money and resources toward cyber security are increasing. These resource allocations are likely to continue and to increase in the coming years, not because the threat is overstated, but because the information and assets once stored in file cabinets and bank vaults have now migrated to digital systems. People can survive without electricity, credit cards, and cell phones and have done so for most of human history, but society has changed. Humans are increasingly living in dense urban environments and heavily reliant on interconnected supply chains to provide food, medicine, and all the other aspects of life that are now largely taken for granted. Would New York City survive a power outage that extends for days on end? Absolutely, but it would not be without consequences and likely deaths. The political ramifications of extensive disruptions of lifestyle due to nonkinetic cyber attacks on critical infrastructure are likely to be as disastrous for those in power as other kinetic incidents.

If war is an inherently political act, then cyber warfare need not be violent to affect the lives of its targets. Its political utility lies in its ability to affect citizenry who by extension demand more of policy-makers. A focus on cyber security should not preempt or preclude concerns of conventional symmetric and asymmetric threats to state survival. Instead, it should be recognized as an extension of the study of security studies. Cyber concerns extend the volume and scale of issues that can affect national security. At the same time it is important to concede that issues in cyberspace can be studied by leveraging many of the tools of the past with modifications to account for many of the novel attributes of cyberspace.

"Cyberspace," a term originating in science fiction, has evolved into concern for science fact. The progress of technology will not wait for advances in theory. The last twenty years alone have seen the extension of cyberspace from millions to billions of connected devices and have enabled everything from the tweeting of covert operations in Abbottabad to the prediction of outcomes of elections based on public sentiment. Technology is not limitless, although it often seems to be. Despite Lawrence Lessig's famous quote, "code is law," code is constantly being rewritten, and loopholes in the form of zero-day exploits and human ignorance and malice are constantly being exploited.[8] The law of cyberspace is changing rapidly and will continue to do so as more and more devices are connected and more and more code is written. Parsimonious models predicated on predicting when and why states and other actors behave the way they do in cyberspace will be increasingly important in helping to shape offensive and defensive strategies that will come to define cyber interactions between states in the decades to come. The theoretical foundation and examined evidence for the ex-

pected utility of international cyber conflict make clear the need for an accurate understanding of both one's own and one's adversaries' capabilities.

Data constraints at present are the most significant roadblock to creating more robust and meaningful models over time and space. These constraints are falling away quickly, and it is likely scholars attempting to make use of new data to examine state-on-state cyber interactions will provide new studies that will build upon the work presented here. It is important that the field not be consumed by studies only constructed with anecdotal evidence or single case studies. To truly make the study of cyber conflict applicable to modern international relations, anecdotal evidence must be supported by rigorous empirical testing.

The body of evidence presented here, although constrained in many ways, offers a glimpse into how states decide to engage in offensive cyber operations. Whether any given state leverages all available data to construct a rational model is of less importance than demonstrating that, knowingly or unknowingly, states are behaving rationally based on the attributes of the argument developed for the expected utility of international cyber conflict. It is possible to walk away from this preliminary attempt understanding that decision-making within cyberspace does not occur within a Wild West frontier existing outside the bounds of rationality or predictable state behavior. Instead, cyberspace is an environment in which actors continue to act rationally within a new set of constraints.

This page intentionally left blank

APPENDIX A

Power Score Components and Scores

Country	MUD	LRF	ESC	TI	IA	MBA	TSC	NDV	Power Score	Weighted Power Score
Argentina	4	5.45	3.71	2.55	1.50	0.05	1.67	3.60	1.33	4.29
Australia	6	8.73	5.95	7.59	6.00	0.33	5	7.60	3.79	8.36
Brazil	6	6.05	3.73	2.23	3.00	0.49	3.33	4.07	2.93	4.58
Canada	6	8.13	5.76	5.76	5.75	0.33	5	8.16	3.24	9.02
China	10	3.25	5.46	3.21	3.00	1.73	5	3.43	6.47	3.58
Estonia	6	9.40	4.29	5.10	5.50	0.00	3.33	7.41	2.27	8.27
France	6	9.25	4.82	4.10	5.75	0.84	5	8.01	3.20	8.89
Georgia	4	3.33	3.00	4.17	1.00	0.00	3.33	2.69	3.20	3.03
Germany	6	10.00	5.06	5.70	3.75	0.64	5	8.20	3.17	9.41
India	8	5.30	2.36	2.10	2.50	0.66	5	0.75	23.24	0.81
Indonesia	0	3.45	3.32	1.36	0.50	0.06	3.33	0.99	4.87	1.33
Iran	4	2.85	2.63	3.96	3.75	0.10	5	1.30	7.38	1.33
Israel	10	9.25	4.75	6.43	5.75	0.20	10	6.72	9.02	7.27
Italy	4	7.73	3.60	4.03	7.25	0.50	3.33	5.37	2.80	5.72
Japan	6	9.08	6.62	3.94	2.25	0.78	3.33	7.82	2.03	9.36
Mexico	4	5.60	4.43	2.01	3.00	0.07	3.33	3.11	3.41	3.63
Russia	8	4.15	3.49	2.26	2.75	0.84	6.67	4.30	2.77	4.57
Saudi Arabia	2	3.18	2.39	2.21	2.25	0.64	3.33	4.10	1.72	4.49
South Africa	2	5.93	3.03	1.80	0.75	0.06	3.33	1.23	6.12	1.57
ROK	6	6.65	5.62	7.03	4.50	0.39	5	8.37	3.01	9.17
Syria	0	1.38	2.46	1.91	1.50	0.03	1.67	2.07	0.98	2.39
Turkey	4	5.45	2.98	1.83	0.75	0.25	3.33	3.98	2.13	4.82
UK	8	10.00	6.35	7.66	6.00	0.83	5	8.50	3.81	9.35
USA	10	10.00	6.40	6.09	5.75	10.00	10	7.40	10.86	7.44

Source: Variables LRF, ESC, TI, and IA are from "Cyber Power Index." NDV is derived from "World Telecommunication/ICT Indicators Database Online." MUD and TSC are from the case studies of national cyber capabilities presented in Billo and Chang, "Cyber Warfare"; Lewis and Timlin, *Cybersecurity and Cyberwarfare*; and Carr, *Cyber Warfare*. MBA information is from "SIPRI Military Expenditure Database."

Variables: Military unit designation* (MUD); legal and regulatory frameworks* (LRF); economic and social context* (ESC); technological infrastructure* (TI); industrial application* (IA); military budget allocation* (MBA); threat spectrum capabilities (TSC); national digital vulnerability (NDV). *indicates weighted variables.

This page intentionally left blank

APPENDIX B

Modified Economist Intelligence Unit Component Values

Duplications in the following appendix are a weighting of values within various categories and are not a repeating of numbers. For instance, within the subcategory of ICT affordability are mobile phone tariffs and broadband tariffs. These two combine to make up the subcategory ICT affordability. Because the secure servers category is independent, its weighted value is placed above it with the * symbol to indicate the within variable weighted value per country. These subcategories can contain other variables.

APPENDIX B Modified Economist Intelligence Unit Component Values

			Argentina	Australia	Brazil
Legal and Regulatory Framework		Total	54.5	87.25	60.5
Commitment to cyber development*		30.00%	15	26.25	22.5
National cyber plan	Rating 0–4 (4=best)	50.00%	50	100	75
Public-private partnerships	Rating 0–4 (4=best)	50.00%	50	75	75
Cyber protection policy*		30.00%	12	21	10.5
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	50	100	50
Cyber security laws	Rating 0–4 (4=best)	20.00%	50	100	50
Cyber crime response	Rating 0–4 (4=best)	20.00%	75	100	50
International cyber security commitments	Rating 0–4 (4=best)	20.00%	25	25	0
Cyber security plan	Rating 0–4 (4=best)	20.00%	0	25	25
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	15	15	15
Cyber censorship	Rating 0–2 (2=Best)	15.00%	100	100	100
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	12.5	25	12.5
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	50	100	50
Economic and Social Context		Total	37.05	59.47	37.34
Educational levels*		25.20%	18.72	17.8	13.96
Tertiary student enrollment	% of gross enrollment	50.00%	92.35	41.25	73.28
Expected years of education	primary to tertiary, in years	50.00%	56.25	100	37.5
Technical skills*		27.40%	10.11	16.76	7.46
Labor productivity growth	% change between 2009 and 2010	25.00%	76.72	15.52	56.9
Researchers in R&D	per million population	25.00%	20.87	90.57	14.75
Science and engineering degrees	% of total degrees	25.00%	0	38.6	12.28
English literacy	Rating 0–4 (4=Best)	25.00%	50	100	25
Trade*		17.30%	6.22	7.62	6.54
ICT exports	% of total exports	33.33%	1.36	4.75	6.1
ICT imports	% of total imports	33.33%	46.67	47.5	47.5

Openness to trade	Rating 1–5 (5=Best)	33.33%	60	80	60
Innovation environment*		30.10%	1.99	17.29	9.38
R&D investment	% of GDP	33.33%	10.64	44.68	23.4
Domestic patent filings	filings per million population	33.33%	8.69	82.83	7.42
Private equity investment	% of GDP	33.33%	0	40	60
Technology Infrastructure		Total	25.46	75.91	22.25
ICT access*		22.00%	10.52	16.31	7.37
Internet penetration	Internet users per 100 people	50.00%	29.7	83.08	25.44
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	65.98	65.15	41.56
ICT quality*		23.00%	3.56	9.27	2.57
Fixed broadband subscribers	% of all Internet subscribers	50.00%	25.21	67.05	17.19
International Internet bandwidth	bits/second/person	50.00%	5.72	13.57	5.19
Telecom investment as % of GDP*	% of GDP	20.00%	6.17	15.37	8.31
Telecom investment as % of GDP	% of GDP	20.00%	30.85	76.84	41.54
ICT affordability*		10.00%	4.75	3.49	3.29
Mobile phone tariffs	PPP $	50.00%	68.92	82.91	19.67
Broadband Internet tariffs	PPP $	50.00%	26.1	–13.21	46.12
Secure servers*	secure servers per million	25.80%	0.45	31.48	0.71
Secure servers	secure servers per million	25.80%	1.75	122.03	2.77
Industry Application		Total	15	60	30
Smart grids	Rating 0–4 (4=best)	60.00%	0	50	25
E-health	Rating 0–4 (4=best)	20.00%	50	75	50
E-government	Rating 0–1 (1=best)	20.00%	25	75	25

(*continued*)

APPENDIX B (continued)

			Canada	China	France
Legal and Regulatory Framework		Total	81.25	32.5	92.5
Commitment to cyber development*		30.00%	26.25	11.25	30
National cyber plan	Rating 0–4 (4=best)	50.00%	75	50	100
Public-private partnerships	Rating 0–4 (4=best)	50.00%	100	25	100
Cyber protection policy*		30.00%	15	15	30
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	50	75	100
Cyber security laws	Rating 0–4 (4=best)	20.00%	75	50	100
Cyber crime response	Rating 0–4 (4=best)	20.00%	50	50	100
International cyber security commitments	Rating 0–4 (4=best)	20.00%	50	50	100
Cyber security plan	Rating 0–4 (4=best)	20.00%	25	25	100
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	15	0	7.5
Cyber censorship	Rating 0–2 (2=Best)	15.00%	100	0	50
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	25	6.25	25
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	100	25	100
Economic and Social Context		Total	57.56	54.6	48.2
Educational levels*		25.20%	10.41	9.55	14.25
Tertiary student enrollment	% of gross enrollment	50.00%	24.25	63.29	53.7
Expected years of education	primary to tertiary, in years	50.00%	58.33	12.5	59.38
Technical skills*		27.40%	18.3	16.86	14.03
Labor productivity growth	% change between 2009 and 2010	25.00%	30.17	98.28	25.86
Researchers in R&D	per million population	25.00%	91.35	22.84	74.93
Science and engineering degrees	% of total degrees awarded	25.00%	45.61	100	54.09
English literacy	Rating 0–4 (4=Best)	25.00%	100	25	50
Trade*		17.30%	8.92	17.28	7.57
ICT exports	% of total exports	33.33%	14.92	100	18.98
ICT imports	% of total imports	33.33%	40	100	32.5

Openness to trade	Rating 1–5 (5=Best)	33.33%	100	100	80
Innovation environment*		30.10%	19.93	10.91	12.34
R&D investment	% of GDP	33.33%	38.3	29.79	42.55
Domestic patent filings	filings per million population	33.33%	74.78	15.86	17.01
Private equity investment	% of GDP	33.33%	80	60	60
Technology Infrastructure		Total	57.63	32.11	40.97
ICT access*		22.00%	13.12	4.67	14.39
Internet penetration	Internet users per 100 people	50.00%	90.85	23.56	79.45
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	28.39	18.87	51.32
ICT quality*		23.00%	14.21	3.01	19.38
Fixed broadband subscribers	% of all Internet subscribers	50.00%	83.09	24.64	95.13
International Internet bandwidth	bits/second/person	50.00%	40.43	1.55	73.37
Telecom investment as % of GDP*	% of GDP	20.00%	2.78	16.47	0.55
Telecom investment as % of GDP	% of GDP	20.00%	13.92	82.34	2.77
ICT affordability*		10.00%	5.41	7.94	1.38
Mobile phone tariffs	PPP $	50.00%	58.46	92.52	7.64
Broadband Internet tariffs	PPP $	50.00%	49.74	66.24	19.94
Secure servers*	secure servers per million	25.80%	22.11	0.02	5.28
Secure servers	secure servers per million	25.80%	85.69	0.08	20.46
Industry Application		Total	57.5	30	57.5
Smart grids	Rating 0–4 (4=best)	60.00%	50	25	50
E-health	Rating 0–4 (4=best)	20.00%	50	50	75
E-government	Rating 0–1 (1=best)	20.00%	87.5	25	62.5

(*continued*)

APPENDIX B (continued)

			Germany	India	Indonesia
Legal and Regulatory Framework		Total	100	53	34.5
Commitment to cyber development*		30.00%	30	15	15
National cyber plan	Rating 0–4 (4=best)	50.00%	100	50	50
Public-private partnerships	Rating 0–4 (4=best)	50.00%	100	50	50
Cyber protection policy*		30.00%	30	10.5	12
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	100	50	75
Cyber security laws	Rating 0–4 (4=best)	20.00%	100	50	50
Cyber crime response	Rating 0–4 (4=best)	20.00%	100	50	75
International cyber security commitments	Rating 0–4 (4=best)	20.00%	100	0	0
Cyber security plan	Rating 0–4 (4=best)	20.00%	100	25	0
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	15	15	7.5
Cyber censorship	Rating 0–2 (2=Best)	15.00%	100	100	50
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	25	12.5	0
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	100	50	0
Economic and Social Context		Total	50.59	23.62	33.19
Educational levels*		25.20%	8.61	2.89	13.71
Tertiary student enrollment	% of gross enrollment	50.00%	9.99	22.96	79.64
Expected years of education	primary to tertiary, in years	50.00%	58.33	0	29.17
Technical skills*		27.40%	18	10.18	6.05
Labor productivity growth	% change between 2009 and 2010	25.00%	41.38	28.45	39.66
Researchers in R&D	per million population	25.00%	75.7	2.78	4.24
Science and engineering degrees	% of total degrees awarded	25.00%	70.76	92.4	44.44
English literacy	Rating 0–4 (4=Best)	25.00%	75	25	0
Trade*		17.30%	9.32	8.62	9.2
ICT exports	% of total exports	33.33%	23.05	12.88	19.32
ICT imports	% of total imports	33.33%	38.75	36.67	40.42

Openness to trade	Rating 1–5 (5=Best)	33.33%	100	100	100
Innovation environment*		30.10%	14.66	1.94	4.22
R&D investment	% of GDP	33.33%	53.19	17.02	0
Domestic patent filings	filings per million population	33.33%	48.82	1.72	0.9
Private equity investment	% of GDP	33.33%	40	0	40
Technology Infrastructure		Total	56.97	21.02	13.57
ICT access*		22.00%	19.06	6.92	2.86
Internet penetration	Internet users per 100 people	50.00%	89.1	1.52	3.88
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	84.19	61.42	22.1
ICT quality*		23.00%	17.55	0.03	0.02
Fixed broadband subscribers	% of all Internet subscribers	50.00%	88.54	0.29	0
International Internet bandwidth	bits/second/person	50.00%	64.11	0	0.2
Telecom Investment as % of GDP*	% of GDP	20.00%	0.05	4.04	2.65
Telecom Investment as % of GDP	% of GDP	20.00%	0.23	20.21	13.25
ICT affordability*		10.00%	4.75	10	8.02
Mobile phone tariffs	PPP $	50.00%	94.07	100	98.76
Broadband Internet tariffs	PPP $	50.00%	0.85	99.99	61.66
Secure servers*	secure servers per million	25.80%	15.57	0.02	0.02
Secure servers	secure servers per million	25.80%	60.33	0.1	0.09
Industry Application		Total	37.5	25	5
Smart grids	Rating 0–4 (4=best)	60.00%	25	25	0
E-health	Rating 0–4 (4=best)	20.00%	75	25	25
E-government	Rating 0–1 (1=best)	20.00%	37.5	25	0

(*continued*)

APPENDIX B (continued)

			Italy	Japan	Mexico
Legal and Regulatory Framework		Total	77.25	90.75	56
Commitment to cyber development*		30.00%	22.5	30	15
National cyber plan	Rating 0–4 (4=best)	50.00%	75	100	50
Public-private partnerships	Rating 0–4 (4=best)	50.00%	75	100	50
Cyber protection policy*		30.00%	21	27	13.5
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	50	100	75
Cyber security laws	Rating 0–4 (4=best)	20.00%	75	100	50
Cyber crime response	Rating 0–4 (4=best)	20.00%	75	100	50
International cyber security commitments	Rating 0–4 (4=best)	20.00%	100	50	25
Cyber security plan	Rating 0–4 (4=best)	20.00%	50	100	25
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	15	15	15
Cyber censorship	Rating 0–2 (2=Best)	15.00%	100	100	100
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	18.75	18.75	12.5
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	75	75	50
Economic and Social Context		Total	35.95	66.23	44.34
Educational levels*		25.20%	12.34	9.67	16.26
Tertiary student enrollment	% of gross enrollment	50.00%	67.7	27.76	92.61
Expected years of education	primary to tertiary, in years	50.00%	30.21	48.96	36.46
Technical skills*		27.40%	8.96	18.72	10.88
Labor productivity growth	% change between 2009 and 2010	25.00%	24.14	53.45	49.14
Researchers in R&D	per million population	25.00%	34.54	119.54	7.41
Science and engineering degrees	% of total degrees awarded	25.00%	47.08	50.29	52.34
English literacy	Rating 0–4 (4=Best)	25.00%	25	50	50
Trade*		17.30%	6.8	9.21	15.25
ICT exports	% of total exports	33.33%	10.17	49.83	77.63
ICT imports	% of total imports	33.33%	27.92	50	87.08

Openness to trade	Rating 1–5 (5=Best)	33.33%	80	60	100
Innovation environment*		30.10%	7.85	28.64	1.95
R&D investment	% of GDP	33.33%	25.53	72.34	10.64
Domestic patent filings	filings per million population	33.33%	10.52	185.07	8.24
Private equity investment	% of GDP	33.33%	40	20	0
Technology Infrastructure		Total	40.27	39.38	20.11
ICT access*		22.00%	16.6	14.92	6.08
Internet penetration	Internet users per 100 people	50.00%	50.13	88.85	23.56
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	100.75	46.77	31.71
ICT quality*		23.00%	10.68	10.25	3.11
Fixed broadband subscribers	% of all Internet subscribers	50.00%	60.46	74.79	26.36
International Internet bandwidth	bits/second/person	50.00%	32.42	14.36	0.7
Telecom Investment as % of GDP*	% of GDP	20.00%	4.72	1.82	2.52
Telecom Investment as % of GDP	% of GDP	20.00%	23.62	9.09	12.62
ICT affordability*		10.00%	5.52	0.79	8.04
Mobile phone tariffs	PPP $	50.00%	71.6	–0.09	90.52
Broadband internet tariffs	PPP $	50.00%	38.83	15.92	70.35
Secure servers*	secure servers per million	25.80%	2.75	11.6	0.35
Secure servers	secure servers per million	25.80%	10.64	44.95	1.38
Industry Application		Total	72.5	22.5	30
Smart grids	Rating 0–4 (4=best)	60.00%	100	0	25
E-health	Rating 0–4 (4=best)	20.00%	50	50	50
E-government	Rating 0–1 (1=best)	20.00%	12.5	62.5	25

(*continued*)

APPENDIX B (continued)

			Russia	Saudi Arabia	South Africa
Legal and Regulatory Framework		Total	41.5	31.75	59.25
Commitment to cyber development*		30.00%	18.75	15	15
National cyber plan	Rating 0–4 (4=best)	50.00%	75	50	75
Public-private partnerships	Rating 0–4 (4=best)	50.00%	50	50	25
Cyber protection policy*		30.00%	9	10.5	10.5
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	75	75	0
Cyber security laws	Rating 0–4 (4=best)	20.00%	25	50	50
Cyber crime response	Rating 0–4 (4=best)	20.00%	50	50	50
International cyber security commitments	Rating 0–4 (4=best)	20.00%	0	0	50
Cyber security plan	Rating 0–4 (4=best)	20.00%	0	0	25
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	7.5	0	15
Cyber censorship	Rating 0–2 (2=Best)	15.00%	50	0	100
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	6.25	6.25	18.75
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	25	25	75
Economic and Social Context		Total	34.86	23.89	30.34
Educational levels*		25.20%	9.27	4.33	7.38
Tertiary student enrollment	% of gross enrollment	50.00%	35.02	0	31.52
Expected years of education	primary to tertiary, in years	50.00%	38.54	34.38	27.08
Technical skills*		27.40%	12.73	10.4	12.22
Labor productivity growth	% change between 2009 and 2010	25.00%	44.83	33.62	55.17
Researchers in R&D	per million population	25.00%	68.38	3.39	8.27
Science and engineering degrees	% of total degrees awarded	25.00%	47.66	89.77	64.91
English literacy	Rating 0–4 (4=Best)	25.00%	25	25	50
Trade*		17.30%	6.74	6.92	7.35
ICT exports	% of total exports	33.33%	2.03	1.02	6.78
ICT imports	% of total imports	33.33%	35	19.17	40.83

Openness to trade	Rating 1–5 (5=Best)	33.33%	80	100	80
Innovation environment*		30.10%	6.11	2.24	3.39
R&D investment	% of GDP	33.33%	21.28	0	19.15
Domestic patent filings	filings per million population	33.33%	17.94	1.66	13.68
Private equity investment	% of GDP	33.33%	20	20	0
Technology Infrastructure		Total	22.61	22.09	17.99
ICT access*		22.00%	12.39	12.19	7.11
Internet penetration	Internet users per 100 people	50.00%	27.94	39.1	5.14
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	84.69	71.69	59.52
ICT quality*		23.00%	3.52	2.04	0.24
Fixed broadband subscribers	% of all Internet subscribers	50.00%	29.23	13.47	2.01
International Internet bandwidth	bits/second/person	50.00%	1.35	4.25	0.1
Telecom investment as % of GDP*	% of GDP	20.00%	–2.06	1.38	3.68
Telecom investment as % of GDP	% of GDP	20.00%	–10.29	6.9	18.39
ICT affordability*		10.00%	8.41	6.19	5.86
Mobile phone tariffs	PPP $	50.00%	88.46	82.25	66.99
Broadband internet tariffs	PPP $	50.00%	79.83	41.48	50.14
Secure servers*	secure servers per million	25.80%	0.35	0.3	1.1
Secure servers	secure servers per million	25.80%	1.36	1.16	4.28
Industry Application		Total	27.5	22.5	7.5
Smart grids	Rating 0–4 (4=best)	60.00%	25	25	0
E-health	Rating 0–4 (4=best)	20.00%	50	25	25
E-government	Rating 0–1 (1=best)	20.00%	12.5	12.5	12.5

(*continued*)

APPENDIX B (continued)

			South Korea	Turkey	United Kingdom
Legal and Regulatory Framework		Total	66.5	54.5	100
Commitment to cyber development*		30.00%	30	15	30
National cyber plan	Rating 0–4 (4=best)	50.00%	100	75	100
Public-private partnerships	Rating 0–4 (4=best)	50.00%	100	25	100
Cyber protection policy*		30.00%	16.5	19.5	30
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	100	75	100
Cyber security laws	Rating 0–4 (4=best)	20.00%	75	75	100
Cyber crime response	Rating 0–4 (4=best)	20.00%	75	75	100
International cyber security commitments	Rating 0–4 (4=best)	20.00%	0	50	100
Cyber security plan	Rating 0–4 (4=best)	20.00%	25	50	100
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	7.5	7.5	15
Cyber censorship	Rating 0–2 (2=Best)	15.00%	50	50	100
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	12.5	12.5	25
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	50	50	100
Economic and Social Context		Total	56.23	29.8	63.52
Educational levels*		25.20%	13.86	10.27	20.08
Tertiary student enrollment	% of gross enrollment	50.00%	42.28	66.93	100
Expected years of education	primary to tertiary, in years	50.00%	67.71	14.58	59.38
Technical skills*		27.40%	19.31	9.24	17.64
Labour productivity growth	% change between 2009 and 2010	25.00%	56.03	37.93	24.14
Researchers in R&D	per million population	25.00%	99.22	14.45	91.53
Science and engineering degrees	% of total degrees awarded	25.00%	76.61	82.46	41.81
English literacy	Rating 0–4 (4=Best)	25.00%	50	0	100
Trade*		17.30%	12.88	6.47	8.81
ICT exports	% of total exports	33.33%	49.49	7.8	29.15
ICT imports	% of total imports	33.33%	94.17	24.58	43.75

Openness to trade	Rating 1–5 (5=Best)	33.33%	80	80	80
Innovation environment*		30.10%	10.18	3.82	16.99
R&D investment	% of GDP	33.33%	68.09	14.89	40.43
Domestic patent filings	filings per million population	33.33%	10.52	2.1	24.14
Private equity investment	% of GDP	33.33%	20	20	100
Technology Infrastructure		Total	70.32	18.27	76.56
ICT access*		22.00%	16.05	9.84	18.63
Internet penetration	Internet users per 100 people	50.00%	93.73	38.6	89.6
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	52.15	50.83	79.8
ICT quality*		23.00%	13.24	4.17	21.55
Fixed broadband subscribers	% of all Internet subscribers	50.00%	100	25.5	88.25
International Internet bandwidth	bits/second/person	50.00%	15.09	10.74	99.16
Telecom Investment as % of GDP*	% of GDP	20.00%	15.04	−2.89	5.95
Telecom Investment as % of GDP	% of GDP	20.00%	75.2	−14.47	29.77
ICT affordability*		10.00%	5.86	5.4	5.49
Mobile phone tariffs	PPP $	50.00%	62.86	41.05	59.31
Broadband Internet tariffs	PPP $	50.00%	54.27	66.97	50.46
Secure servers*	secure servers per million	25.80%	20.14	1.76	24.93
Secure servers	secure servers per million	25.80%	78.06	6.8	96.61
Industry Application		Total	45	7.5	60
Smart grids	Rating 0–4 (4=best)	60.00%	25	0	50
E-health	Rating 0–4 (4=best)	20.00%	50	25	75
E-government	Rating 0–1 (1=best)	20.00%	100	12.5	75

(*continued*)

APPENDIX B (continued)

			United States	Israel	Syria
Legal and Regulatory Framework		Total	100	92.5	13.75
Commitment to cyber development*		30.00%	30	30	0
National cyber plan	Rating 0–4 (4=best)	50.00%	100	100	0
Public-private partnerships	Rating 0–4 (4=best)	50.00%	100	100	0
Cyber protection policy*		30.00%	30	22.5	7.5
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	100	100	75
Cyber security laws	Rating 0–4 (4=best)	20.00%	100	75	25
Cyber crime response	Rating 0–4 (4=best)	20.00%	100	100	25
International cyber security commitments	Rating 0–4 (4=best)	20.00%	100	0	0
Cyber security plan	Rating 0–4 (4=best)	20.00%	100	100	0
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	15	15	0
Cyber censorship	Rating 0–2 (2=Best)	15.00%	100	100	0
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	25	25	6.25
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	100	100	25
Economic and Social Context		Total	63.95	47.54	24.58
Educational levels*		25.20%	15.01	6.74	9.63
Tertiary student enrollment	% of gross enrollment	50.00%	60.83	0.389	67.06
Expected years of education	primary to tertiary, in years	50.00%	58.33	53.13	9.38
Technical skills*		27.40%	18.47	15.87	9.65
Labor productivity growth	% change between 2009 and 2010	25.00%	45.69	31.9	91.38
Researchers in R&D	per million population	25.00%	100	33.56	0.46
Science and engineering degrees	% of total degrees awarded	25.00%	23.98	91.23	23.98
English literacy	Rating 0–4 (4=Best)	25.00%	100	75	25
Trade*		17.30%	11.92	9.2	5.09
ICT exports	% of total exports	33.33%	44.07	41.69	0
ICT imports	% of total imports	33.33%	62.92	37.92	8.33

Openness to trade	Rating 1–5 (5=Best)	33.33%	100	80	80
Innovation environment*		30.10%	18.54	15.73	0.22
R&D investment	% of GDP	33.33%	59.57	100	2.13
Domestic patent filings	filings per million population	33.33%	100.05	12.42	0
Private equity investment	% of GDP	33.33%	20	40	0
Technology Infrastructure		Total	60.87	64.26	19.1
ICT access*		22.00%	16.36	18.01	4.75
Internet penetration	Internet users per 100 people	50.00%	101.25	78.57	20.3
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	47.52	85.18	22.85
ICT quality*		23.00%	12.07	19.51	4.42
Fixed broadband subscribers	% of all Internet subscribers	50.00%	76.79	69.63	24.16
International Internet bandwidth	bits/second/person	50.00%	28.14	100	14.27
Telecom investment as % of GDP*	% of GDP	20.00%	–0.01	11.18	4.13
Telecom investment as % of GDP	% of GDP	20.00%	–0.07	55.92	20.65
ICT affordability*		10.00%	6.65	8.49	5.8
Mobile phone tariffs	PPP $	50.00%	73.2	72.99	26.99
Broadband Internet tariffs	PPP $	50.00%	59.76	96.74	89.09
Secure servers*	secure servers per million	25.80%	25.8	7.07	0
Secure servers	secure servers per million	25.80%	100	27.41	0
Industry Application		Total	57.5	57.5	15
Smart grids	Rating 0–4 (4=best)	60.00%	50	50	0
E-health	Rating 0–4 (4=best)	20.00%	50	50	0
E-government	Rating 0–1 (1=best)	20.00%	87.5	87.5	75

(*continued*)

APPENDIX B (continued)

			Estonia	Iran	Georgia
Legal and Regulatory Framework		Total	94	28.5	33.25
Commitment to cyber development*		30.00%	30	15	7.5
National cyber plan	Rating 0–4 (4=best)	50.00%	100	25	25
Public-private partnerships	Rating 0–4 (4=best)	50.00%	100	75	25
Cyber protection policy*		30.00%	24	13.5	12
Cyber enforcement authority	Rating 0–4 (4=best)	20.00%	75	75	0
Cyber security laws	Rating 0–4 (4=best)	20.00%	75	75	25
Cyber crime response	Rating 0–4 (4=best)	20.00%	50	50	50
International cyber security commitments	Rating 0–4 (4=best)	20.00%	100	0	100
Cyber security plan	Rating 0–4 (4=best)	20.00%	100	25	25
Cyber censorship*	Rating 0–2 (2=Best)	15.00%	15	0	7.5
Cyber censorship	Rating 0–2 (2=Best)	15.00%	100	0	50
Intellectual property protection*	Rating 0–4 (0=Best)	25.00%	25	0	6.25
Intellectual property protection	Rating 0–4 (0=Best)	25.00%	100	0	25
Economic and Social Context		Total	42.88	26.34	29.96
Educational levels*		25.20%	13.04	7.71	15.18
Tertiary student enrollment	% of gross enrollment	50.00%	48.25	37.22	92.35
Expected years of education	primary to tertiary, in years	50.00%	55.21	23.96	28.13
Technical skills*		27.40%	17.11	11.94	7.58
Labor productivity growth	% change between 2009 and 2010	25.00%	55.17	0	52.59
Researchers in R&D	per million population	25.00%	53.45	15.97	0
Science and engineering degrees	% of total degrees awarded	25.00%	91.23	133.33	33.1
English literacy	Rating 0–4 (4=Best)	25.00%	50	25	25
Trade*		17.30%	7.86	4.61	6.52
ICT exports	% of total exports	33.33%	26.44	0	0.68
ICT imports	% of total imports	33.33%	30	0	32.5
Openness to trade	Rating 1–5 (5=Best)	33.33%	80	80	80

Innovation environment*		30.10%	4.87	2.08	0.67
R&D investment	% of GDP	33.33%	23.4	14.89	4.26
Domestic patent filings	filings per million population	33.33%	3.79	5.28	2.27
Private equity investment	% of GDP	33.33%	20	0	0
Technology Infrastructure		Total	51.02	39.61	41.69
ICT access*		22.00%	18.05	6.73	8.67
Internet penetration	Internet users per 100 people	50.00%	87.09	10.65	28.07
Mobile cellular penetration	mobile cellular subscriptions per 100 people	50.00%	76.99	50.5	50.75
ICT quality*		23.00%	14.62	11.92	8.83
Fixed broadband subscribers	% of all Internet subscribers	50.00%	69.63	28.65	14.33
International Internet bandwidth	bits/second/person	50.00%	57.47	74.98	62.47
Telecom investment as % of GDP*	% of GDP	20.00%	4.99	14.64	20
Telecom investment as % of GDP	% of GDP	20.00%	24.95	73.19	100
ICT affordability*		10.00%	5.62	6.33	3.99
Mobile phone tariffs	PPP $	50.00%	70.7	94.95	79.75
Broadband Internet tariffs	PPP $	50.00%	41.77	31.56	–0.02
Secure servers*	secure servers per million	25.80%	7.74	0	0.2
Secure servers	secure servers per million	25.80%	30.02	0	0.77
Industry Application		Total	55	37.5	10
Smart grids	Rating 0–4 (4=best)	60.00%	50	50	0
E-health	Rating 0–4 (4=best)	20.00%	50	0	0
E-government	Rating 0–1 (1=best)	20.00%	75	37.5	50

Data for all countries except Georgia, Iran, Israel, Syria, and Estonia are from "Cyber Power Index." The five additional countries include data from the same sources as the EIU data including Billo and Chang, "Cyber Warfare"; Lewis and Timlin, *Cybersecurity and Cyberwarfare*; Carr, *Cyber Warfare*; Kelly and Cook, "Freedom on the Net 2011"; United Nations, UNESCO Institute for Statistics, "United Nations Commodity Trade Statistics Database"; World Bank, World Development Indicators; United Nations, Public Administration Network, "2012 Global E-Government Survey." Several of the variables included in the "Cyber Power Index" were omitted due to data limitations across nations. All data from the newly added countries were included from the most recent year to date with available data from the same sources as used by the Economist Intelligence Unit to maintain consistency. Where variables were dropped, the weighting percentages were proportionally distributed.

* denotes the weighted subcategories that make up a variable.

This page intentionally left blank

APPENDIX C

Affinity Scores

Instigator	Target	Year	Type	t – 2	t – 1	Difference in Affinity
China	USA	2006	CE	–0.69	–0.71	0.02
China	UK	2006	Equipment disruption	0.17	0.19	–0.02
Russia	Estonia	2007	DDoS	0.55	0.51	0.04
China	UK	2007	CE	0.19	0.27	–0.08
China	France	2007	CE	0.25	0.28	–0.03
China	Germany	2007	CE	0.41	0.42	–0.01
Israel	Syria	2007	Critical infrastructure disruption	–0.52	–0.44	–0.08
China	France	2007	CE	0.25	0.28	–0.03
China	UK	2007	CE	0.27	0.18	0.09
China	ROK	2008	CE	0.49	0.49	0
China	India	2008	CE	0.82	0.8	0.02
Russia	Georgia	2008	DDoS	0.52	0.49	0.03
China	Canada	2009	CE	0.13	0.11	0.02
China	ROK	2009	CE	0.49	0.46	0.03
China	India	2010	CE	0.76	0.81	–0.05
Iran	China	2010	Website defacement	0.9	0.93	–0.03
China	Australia	2010	CE	0.13	0.1	0.03
China	India	2010	CE	0.76	0.81	–0.05
U.S.	Iran	2010	Compromised hardware systems	–0.71	–0.64	–0.07
Israel	Iran	2010	Compromised hardware systems	–0.41	–0.59	0.18
China	Canada	2011	CE	0	0.06	–0.06
China	ROK	2011	CE	0.39	0.44	–0.05
China	Japan	2011	CE	0.42	0.46	–0.04
Israel	Iran	2011	CE	–0.59	–0.63	0.04
U.S. or Israel	Iran	2011	CE	–0.65	–0.57	–0.08

Source: Strezhnev and Voeten, "United Nations General Assembly Voting Data."

This page intentionally left blank

NOTES

Chapter 1. Introduction to Cyber Decision-Making

1. Cerf, "Day the Internet Age Began"; Hafner, "Laurels for Giving the Internet."

2. C. Metz, "Why Do We Call Them?"; "Paul Baran and the Origins." TCP/IP stands for Transmission Control Protocol/Internet Protocol.

3. Abbate, *Inventing the Internet*.

4. Gibson, *Neuromancer*.

5. Firmware is a term often used to denote the fixed, usually rather small, programs and data structures that internally control various electronic devices. Software is a collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it.

6. Hardware are component devices that are typically installed into or peripheral to a computer case to create a computer upon which system software is installed, including a firmware interface such as a BIOS and an operating system supporting application software that performs the operator's desired functions.

7. Conkey, Williamson, and Simpson, "Washington Metro Delayed Upgrades."

8. U.S. Homeland Security, *National Strategy to Secure Cyberspace*; Kramer, Starr, and Wentz, *Cyberpower and National Security*, 193.

9. Kramer, Starr, and Wentz, *Cyberpower and National Security*.

10. Ibid.; see Kuehl, qtd. on 28.

11. Simpson and Weiner, *Oxford English Dictionary*.

12. Ibid.

13. Ibid.

14. U.S. Strategic Command, "Cyber Warfare Lexicon," 8.

15. Costigan and Perry, *Cyberspaces and Global Affairs*. See chap. 1 for relevant discussions.

16. Black, *War and the World*.

17. Ibid.

18. Ibid.

19. See chap. 2 in Dockrill and French, *Strategy and Intelligence*.

20. Kahn, "Intelligence Failure of Pearl Harbor."

21. Savio, "Browsing History."

22. See chap. 18 in Arquilla and Ronfeldt, *In Athena's Camp*.

23. See particularly the introduction on the role of information in warfare in E. Waltz, *Information Warfare*; see books 1 and 12 on spying, knowledge, and information and the benefits they bring to a leader in Kautalya and Rangarajan, *Arthashastra*.

24. Nye, *Future of Power*.

25. U.S. Defense, "Department of Defense Strategy," 1.

26. Jackson, "Google."

27. Campen, *First Information War*.

28. Libicki, *What Is Information Warfare?*

29. Halpin, *Cyberwar, Netwar and the Revolution*.

30. Lonsdale, *Nature of War*.

31. Owen, Dam, and Lin, *Technology, Policy, Law, and Ethics*.

32. Samaan, "Cyber Command."

33. Eriksson and Giacomello, "Information Revolution, Security, and International Relations." Neorealism as a paradigm assumes an anarchic self-help environment with no governing authority in which states compete to survive. This results in a variety of buttressing theories ranging to include balance of threat and balance of power. States are fundamentally constrained in a competition focused primarily on relative gains rather than on absolute gains.

34. Neoliberalism as a paradigm assumes many of the same features as neorealism, but instead of the assumption that relative gains are paramount to international relations, it is assumed that states can engage in cooperative behavior because of absolute gains.

35. Constructivism in contrast to neorealism and neoliberalism assumes that interactions in international relations are the result of socially constructed patterns of behavior often referred to as norms. The descriptions of neorealism, neoliberalism, and constructivism are simplifications and should not be construed as all-inclusive definitions.

36. Mearsheimer, *Tragedy of Great Power Politics*.

37. Wendt, "Constructing International Politics."

38. Halpin, *Cyberwar, Netwar and the Revolution*.

39. Ibid.

40. Clinton, "Conference on Internet Freedom"; Pleming, "U.S. State Department Speaks to Twitter."

41. Brantly, "Changed Conversation about Surveillance Online."

42. Nye, *Future of Power*, 19.

43. Ibid.

44. Faucon, "New Sanctions Target Iran Oil Sales."

45. Fung, "How to Talk about Blowing Things Up."

46. See two articles dealing with aspects of espionage in the context of legal issues: Katyal, "Criminal Law in Cyberspace"; Shackelford, "From Nuclear War to Net War."

47. Blainey, *Causes of War*; Van Evera, *Causes of War*.

48. K. N. Waltz, *Theory of International Politics*; Mearsheimer, *Tragedy of Great Power Politics*; Keohane, *After Hegemony*; Moravcsik, "Taking Preferences Seriously"; Levy, "Misperception and the Causes of War."

49. Keohane and Nye, *Power and Interdependence*.

50. Clausewitz, Howard, and Paret, *On War*, 39.

51. Von Neumann and Morgenstern, *Theory of Games and Economic Behavior*.

52. Arrow, "Difficulty in the Concept."

53. Nakashima, "List of Cyber-Weapons." This article indicates that the DoD is establishing a decision-making chain of command for cyber actions with hostile intent that need presidential authorization.

54. Bueno De Mesquita, *War Trap*.

55. Ibid., chap. 2.

56. Ibid.

57. Singer, "Reconstructing the Correlates."

58. Potter and Nakao, "Mobitopolo." Potter and Nakao illustrate that the migration of virtual machines across networks can be routed in ways that are more efficient than current technological protocols. In so doing they illustrate that it is possible to map out more efficient

routes on the Internet. This indicates that all actions in cyberspace are not instantaneous and can be manipulated to speed or slow data flow.

59. Fair, "Drone Wars."

60. S. 773, 111th Cong.; the Cybersecurity Act of 2010 was last reported to committee on March 24, 2010. No vote has currently taken place.

Chapter 2. The Key Concepts of Cyber

1. Keohane and Nye, *Power and Interdependence*.

2. Benkler, *Wealth of Networks*.

3. Drezner and Farrell, "Web of Influence."

4. Information communications technologies are a large component of cyberspace. They do not constitute the entirety of the domain, yet they are the most recognizable in most instances.

5. Miard, "Call for Power?"

6. Chickering, "Civil Society and Counterinsurgency."

7. D. L. Wheeler, "Information (without) Revolution?"

8. Pleming, "U.S. State Department Speaks to Twitter."

9. Tor, https://www.torproject.org; Tails, https://tails.boum.org.

10. The Guardian Project, https://guardianproject.info.

11. Lord, *Perils and Promise of Global Transparency*.

12. Ibid, 128–129.

13. Friedman, *Lexus and the Olive Tree*; Friedman, *World Is Flat*.

14. Brynjolfsson and Kahin, "Understanding the Digital Economy."

15. Ibid.

16. Sabourin and Serval, "Electronization of Nasdaq," 588–616.

17. Jones, Kovacich, and Luzwick, *Global Information Warfare*, 87.

18. McCarthy, "Cyberpower and Critical Infrastructure Protection," 550.

19. Ziobro and Yadron, "Target Now Says 70 Million People."

20. Riley et al., "Missed Alarms"; Skariachan and Finkle, "Target Shares Recover"; McGrath, "Target Profit Falls 46%."

21. This estimate was derived by examining the market capitalization of Target immediately prior and three months following the acknowledgment of a significant data breach.

22. "Target Data Breach Cost."

23. J. Brenner, *America the Vulnerable*.

24. Fishman, *Wal-Mart Effect*.

25. "E-Stats, 2014 E-commerce Multi-sector Report."

26. Dearth, "Operationalizing Information Operations," 104.

27. Alberts, *Understanding Information Age Warfare*, 36.

28. Campen, *First Information War*.

29. U.S. Dept. of Defense, "Joint Vision 2020."

30. Ibid.

31. Martin, *Top Secret Intranet*.

32. Cullather, "Bombing at the Speed of Thought."

33. Cooper, "Another View of the Revolution."

34. "Future of the Electric Grid."

35. Lynn, "Defending a New Domain," 98.

36. Alexander, "Building a New Command."
37. J. Brenner, *America the Vulnerable*.
38. Bruner and Suter, *International CIIP Handbook 2008/2009*.
39. S. Metz and Johnson, *Asymmetry and U.S. Military Strategy*.
40. Zero-day exploits are previously unknown vulnerabilities within software that even the vendor of the software is unaware of. These vulnerabilities expose software to exploitation.
41. J. Brenner, *America the Vulnerable*.
42. Cornish et al., "On Cyber Warfare."
43. Arquilla, *Insurgents, Raiders, and Bandits*.
44. Kshetri, "Information and Communications Technologies," 574.
45. Thornton, *Asymmetric Warfare*, 55.
46. Zimet and Barry, "Military Service Overview," 285.
47. Nazario, "Politically Motivated Denial of Service Attacks."
48. Lomsadz, "Shovel Cuts Off Armenia's Internet."
49. Markoff, "Ideas & Trends."
50. Goodman, "Cyber Deterrence."
51. Thomas, "Nation-State Cyber Strategies," 468.
52. D. J. Clark and Konrad, "Asymmetric Conflict," 464.

Chapter 3. The Motivation and Utility for Covert Action

Chapter epigraph is from Einstein and Calaprice, *The New Quotable Einstein*, 173.
1. Fearon, "Rationalist Explanations for War."
2. Ibid.
3. Simon, "Human Nature in Politics," 294.
4. See K. N. Waltz, *Theory of International Politics*, for discussions on anarchy; see Doyle and Macedo, *Striking First*, for a discussion on why preemptive war is not a rational path for war instigation; see Bueno De Mesquita, "Expected Utility Theory," for a discussion on utility and conflict.
5. Fearon, "Rationalist Explanations for War," 386.
6. Bueno De Mesquita, *War Trap*.
7. In the abstract Bueno de Mesquita states explicitly, "An expected utility theory of necessary, but not sufficient, conditions for the initiation and escalation of serious international conflicts, including war, is proposed." Bueno De Mesquita, "Expected Utility Theory."
8. Arrow, "Difficulty in the Concept of Social Welfare."
9. Bueno De Mesquita, *War Trap*, 31.
10. Fearon, "Rationalist Explanations for War," 386.
11. Ibid., 404.
12. Ibid., 382.
13. *i's* perception of anticipated change in the difference between *i's* policies and *j's* policies over the period *t*0(the present) to some future time ($t + n$).
14. See Stein, "Coordination and Collaboration," 41.
15. Ibid.
16. Fishburn, "Utility Theory," 1.
17. "Politics," in *Merriam Webster* (2012).
18. Von Neumann and Morgenstern, *Theory of Games and Economic Behavior*.
19. Downs, *Economic Theory of Democracy*.

20. Ibid., 36.
21. Ibid.
22. Janis and C. R. M. Productions, "Group Dynamics Groupthink"; Kahneman and Tversky, "Prospect Theory."
23. Grafstein, "Rationality as Conditional Expected Utility Maximization."
24. National Security Act of 1947.
25. Lowenthal, *Intelligence*; Johnson, *America's Secret Power*.
26. Treverton, *Covert Action*, 12.
27. Johnson, *America's Secret Power*, 103.
28. Rohde, "Obama Doctrine."
29. Johnson, *America's Secret Power*, 17.
30. Clarridge and Diehl, *Spy for All Seasons*, 42.
31. Olson, *Fair Play*, digital location 791.
32. Shackley and Finney, *Spymaster*, digital location 658.
33. Johnson, *Threat on the Horizon*, digital location 10752.
34. Quoted in Daugherty, *Executive Secrets*, 9.
35. The primary accounting for my mini-case comes from the memoir of Milt Bearden. Bearden and Risen, *Main Enemy*; Daugherty, *Executive Secrets*.
36. Skoudis, "Information Security Issues in Cyberspace," 177–178.
37. Demchak, *Wars of Disruption and Resilience*; Clarke and Knake, *Cyber War*.
38. "Cyberwar: War in the Fifth Domain."
39. Clarke and Knake, *Cyber War*, digital pages 12–26.
40. Ibid.
41. Fuhrmans, "Virus Attacks Siemens."
42. "Cyber-Missile Aimed at Iran?"
43. Broad, Markoff, and Sanger, "Israeli Test on Worm."
44. Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."
45. Worth, "Iranian Supreme Leader."
46. Albright and Brannan, "ISIS Imagery Brief."
47. "Iran Confirms Stuxnet Worm."
48. Sanger, "Obama Order Sped Up Wave."
49. Sanger, *Confront and Conceal*.
50. Ibid. For further information on Stuxnet, Kim Zetter provides an extremely well researched and nuanced account of the malware, its development, and its discovery in her book *Countdown to Zero Day*.
51. McClure, "Operation Cleaver."
52. Barnes and Gorman, "U.S. Says Iran Hacked Navy Computers."
53. Ibid.
54. McClure, "Operation Cleaver," 14.
55. Finkle, "FBI Warns."
56. McClure, "Operation Cleaver," 14.
57. McClure, "Operation Cleaver," 64.

Chapter 4. Digital Power

Chapter epigraph is from Jefferson, *Writings of Thomas Jefferson*, 308.
1. Hart, "Information and Communications Technologies," 204.

2. Weber, quoted by Steven Lukes in Hart, "Information and Communications Technologies," 204.

3. Thucydides, Warner, and Finley, *History of the Peloponnesian War*.

4. Black, *War and the World*.

5. Nye, *Future of Power*.

6. Kramer, Starr, and Wentz, *Cyberpower and National Security*, 38.

7. United States Strategic Command, "Cyber Warfare Lexicon."

8. Nye, "Cyber Power."

9. Billo and Chang, "Cyber Warfare"; Lewis, and Timlin, "Cybersecurity and Cyberwarfare"; "Cyber Power Index."

10. "Cyber Power Index."

11. Singer, "Reconstructing the Correlates."

12. Ibid.."

13. See the inclusion of military personnel in Singer, Bremer, and Stuckey, "Capability Distribution"; Singer, "Reconstructing the Correlates."

14. Lewis and Timlin, *Cybersecurity and Cyberwarfare*.

15. "Cyber Power Index."

16. See appendix B.

17. Lewis and Timlin, *Cybersecurity and Cyberwarfare*; "Cyber Power Index." See appendix B for a more detailed explanation of this variable.

18. "Cyber ShockWave."

19. U.S. Government Accountability Office, "Cybersecurity."

20. "Cyber Power Index."

21. Billo and Chang, "Cyber Warfare."

22. Lewis and Timlin, "Cybersecurity and Cyberwarfare"; Grauman, "Cyber-Security"; Lewis, "Significant Cyber Incidents since 2006"; Billo and Chang, "Cyber Warfare"; Carr, *Cyber Warfare*.

23. Abrams and Weiss, "Malicious Control System Cyber Security."

24. Keeney and Kowalski, "Insider Threat Study."

25. "Defense Critical Infrastructure."

26. Landler and Markoff, "Digital Fears."

27. "World Telecommunication/ICT Indicators Database Online."

28. Bueno De Mesquita, *War Trap*.

Chapter 5. Anonymity and Attribution in Cyberspace

The second epigraph is from "We Are Anonymous, We Are Legion To."

1. "Anonymous," in *Merriam-Webster* (2012), http://www.merriam-webster.com/dictionary/anonymous.

2. S. W. Brenner, "At Light Speed."

3. U.S. Dept. Homeland Security, *National Strategy to Secure Cyberspace*.

4. J. Brenner, *America the Vulnerable*, kindle digital location 1227.

5. Healey, *Fierce Domain*, Kindle digital location 3916.

6. "Anonymous 'Takes Down' CIA Website."

7. D. A. Wheeler and Larsen. "Techniques for Cyber Attack Attribution"; Hunker, Hutchinson, and Margulies, "Role and Challenges."

8. Brantly, "DDoS Mitigation 101."

9. Farivar, "US Indicts Suspected Anonymous Members."

10. Axelrod and Illiev, "Timing of Cyber Conflict."
11. Bilge and Dumitras, "Before We Knew It," 2.
12. Cornish et al., "On Cyber Warfare," 8.
13. Sanger, *Confront and Conceal*.
14. S. W. Brenner, "At Light Speed," 381.
15. Rid, "Cyber War Will Not Take Place," 5.
16. Ibid., 11–12.
17. Kramer, Starr, and Wentz, *Cyberpower and National Security*; Demchak, *Wars of Disruption and Resilience*.
18. See debate in Arquilla, "Cyberwar Is Already Upon Us," and Rid, "Think Again."
19. Bueno De Mesquita, *War Trap*.
20. D. A. Wheeler and Larsen, "Techniques for Cyber Attack Attribution."
21. J. Brenner, *America the Vulnerable*, Kindle digital location 2186.
22. See proposed bill by Joseph Lieberman, "S. 3480 (111th): Protecting Cyberspace as a National Asset Act of 2010," U.S. Senate (Washington, D.C., 2010). The bill was killed in committee.
23. Geers, "Challenge of Cyber Attack Deterrence," 302.

Chapter 6. Cyber and Conventional Operations

1. Giulio Douhet, an Italian general, is widely considered to be the father of theories of airpower and strategy.
2. Clausewitz, Howard, and Paret, *On War*, 92.
3. Ibid., 88.
4. Angstrom and Duyvesteyn, "Understanding Victory and Defeat."
5. Zelizer, *Arsenal of Democracy*.
6. U.S. Dept. of Justice, "President's Constitutional Authority."
7. Singer, "Reconstructing the Correlates."
8. Ibid.
9. Gartzke, "War Is in the Error Term."
10. Pape, "True Worth of Airpower."
11. Ibid.
12. Horowitz and Reiter, "When Does Aerial Bombing Work?"
13. Press, "Myth of Airpower."
14. Campen, *First Information War*.
15. Clarke and Knake, *Cyber War*.
16. U.S. Dept. of Defense, "Military Power of the People's Republic of China."
17. Fisher, "Cyber Warfare Challenges."
18. Thomas, "Cyber Mobilization."
19. Sharma, "Cyber Wars."
20. Ibid.
21. See O'Mahony, "Stuxnet Worm"; IAEA, "Nuclear Verification"; IAEA, "Implementation of the NPT Safeguards Agreement," 73. It should also be noted that the IAEA does not list any on-the-ground inspections within the Islamic Republic of Iran since June 2010 as Stuxnet was being discovered. Furthermore, the assertion that the cyber weapon system was of little to no effect by the Iranians serves direct foreign policy goals and runs counter to discussions held with various government officials.

22. Horowitz and Reiter, "When Does Aerial Bombing Work?"
23. J. Brenner, *America the Vulnerable*.

Chapter 7. Defining the Role of Intelligence in Cyberspace

1. Owen, Dam, and Lin. *Technology, Policy, Law, and Ethics*.
2. See chap. 3, proposition 14 in Gill, Marrin, and Phythian, *Intelligence Theory*.
3. Warner, "Wanted."
4. Alexander, "Building a New Command";Lewis, "Securing Cyberspace for the 44th Presidency"; W. K. Clark and Levin, "Securing the Information Highway"; Geer, "Cybersecurity and National Policy."
5. Alexander, "Building a New Command."
6. Libicki, *Cyberdeterrence and Cyberwar*.
7. Cullather, "Bombing at the Speed of Thought."
8. Herman, "Counter-Terrorism, Information Technology."
9. Ibid.
10. Amoroso, *Cyber Attacks*.
11. Bedi, "Mumbai Attacks."
12. Brantly, "Financing Terror Bit by Bit."
13. J. Brenner, *America the Vulnerable*.
14. P. Williams, Shimeal, and Dunlevy, "Intelligence Analysis for Internet Security."
15. Office of the National Counterintelligence Executive, "Foreign Spies."
16. B. T. Williams, "Joint Force Commander's Guide."
17. Rumsfeld, "DoD News Briefing."
18. An air gap is a security measure often taken for computers and computer networks that must be extraordinarily secure ensuring that a network is physically, electrically, and electromagnetically isolated from insecure networks, such as the public Internet or an insecure local area network. This often includes creating a network with independent electric supplies from public utilities.
19. P. Williams, Shimeal, and Dunlevy, "Intelligence Analysis for Internet Security."
20. E. Waltz, *Information Warfare*.
21. See chap. 8 in Gill, Marrin, and Phythian, *Intelligence Theory*.
22. Pillar, *Intelligence and U.S. Foreign Policy*.
23. Clarke and Knake, *Cyber War;* see chap. 2 of Arquilla and Ronfeldt, *In Athena's Camp*.
24. Rid, *Cyber War Will Not Take Place*.
25. See chap. 8 in Gill, Marrin, and Phythian, *Intelligence Theory*.
26. Ibid.
27. E. Waltz, *Information Warfare*.
28. Ibid.
29. E. Waltz, *Information Warfare*.
30. E. Waltz, *Information Warfare*.
31. Amoroso, *Cyber Attacks*.
32. Gorman and Barnes, "Cyber Combat."
33. Lemos, "In Case of Cyber Attack."
34. Anders Rasmussen (NATO general secretary) in question and answer session with the author following a talk at the United States Military Academy, October 8, 2014.
35. S. W. Brenner, "At Light Speed."

36. Mazanec, "Art of (Cyber) War."
37. Schmitt, *Tallinn Manual*.
38. Falliere, Murchu, and Chien, "W32.Stuxnet Dossier."
39. The PLCs affected were Siemens S7-315 and S7-417. Shakarian, "Stuxnet."
40. Reagan, "Executive Order 12333."
41. Nakashima, "White House."
42. Ibid.
43. Axelrod and Iliev, "Timing of Cyber Conflict."
44. Stokes, Lin, and Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure."
45. D. J. Clark and Konrad, "Asymmetric Conflict."
46. Klimburg, "Mobilising Cyber Power."
47. Landler and Markoff, "Digital Fears"; "Europe: A Cyber-Riot."
48. Traynor, "Russia Accused of Unleashing Cyberwar."
49. Klimburg, "Mobilising Cyber Power."
50. Krekel, "Capability."
51. J. Brenner, *America the Vulnerable*.
52. Greenwald, MacAskill, and Poitras. "Edward Snowden."
53. Strohm and Del Quentin, "Pentagon."
54. Keeney and Kowalski, "Insider Threat Study."
55. U.S. Dept. of Defense, "Joint Doctrine for Electronic Warfare."
56. Sec 1.7(a)(4), in Reagan, "Executive Order 12333."

Chapter 8. How Actors Decide to Use Cyber—a Rational Choice Approach

1. Von Neumann and Morgenstern, *Theory of Games and Economic Behavior*.
2. Bueno de Mesquita, "Contribution of Expected Utility Theory."
3. As is noted by Bueno de Mesquita and others, there are cognitive dimensions of choice that can influence this aspect of rationality as demonstrated in Kahneman and Tversky, "Prospect Theory."
4. Arrow, "Difficulty in the Concept."
5. Bueno De Mesquita, *War Trap*, 118.
6. Bueno De Mesquita, "Expected Utility Theory," 922.
7. Quiggin, *Generalized Expected Utility Theory*, 57.
8. Strezhnev and Voeten, "United Nations General Assembly."
9. Bueno De Mesquita, "Expected Utility Theory," 919.
10. Ibid.
11. Ibid., 920.
12. Bueno De Mesquita, *War Trap*, 47.
13. Ibid.
14. Bueno De Mesquita, "Expected Utility Theory," 925.
15. Singer, Bremer, and Stuckey, "Capability Distribution."
16. Bueno De Mesquita, "Expected Utility Theory," 922.
17. Kramer, Starr, and Wentz, *Cyberpower and National Security*; Nye, "Cyber Power"; Betz and Stevens, *Cyberspace and the State*.
18. Bueno De Mesquita, "Expected Utility Theory," 919. Note that there is no inclusion in this book of his other models illustrating the inclusion of the other five national types.

Because cyberspace operations are largely bilateral ventures, this book focuses on bilateral conflict initiation and utility.

19. Ibid.

20. Ibid.; Organski and Kugler, *War Ledger*.

21. Bueno De Mesquita, "Expected Utility Theory," 924. Note that this is Bueno de Mesquita's fourth proposition, not his third. *Proposition 3* does not apply in the context of cyber as it deals with alliances.

22. Ibid.

23. Ibid.

24. "Cyber Power Index."

25. Lewis, "Significant Cyber Incidents."

26. Ibid.

27. Bueno De Mesquita, *War Trap*.

28. McElroy and Williams, "Flame." Flame constituted a significant virus package identified in multiple systems across the Middle East. The virus was capable of manipulating multiple aspects of the systems it was designed to target.

29. Sanger, *Confront and Conceal*.

30. Bueno De Mesquita, "Expected Utility Theory."

Chapter 9. Cognitive Processes and Decision-Making in Cyberspace

1. Kahneman and Tversky, "Prospect Theory," 263–291.

2. Berejikian, "Cognitive Theory of Deterrence," 181–182.

3. Jervis, "Political Implications of Loss Aversion," 187–204.

4. Ibid., 190.

5. Krebs and Rapport, "International Relations," 530–543.

6. Streich and Levy, "Time Horizons," 200.

7. Liberman and Trope, "Role of Feasibility," 5–18; see also L. E. Williams, Stein, and Galguera, "Distinct Affective Consequences."

8. Trope and Liberman, "Construal-Level Theory," 440.

9. McClure, "Operation Cleaver," 8.

10. Henderson et al., "Construal Level Theory," 165–173.

11. Lindsay and Kello, "Correspondence," 181–192.

12. Jiga-Boy, Clarke, and Semin, "Situating Construal Level," 201–221.

13. Wortzel, "Assessing the Chinese Cyber Threat," 1–6; Minnick, "Experts."

14. Lewis, "Asia."

15. Lardner, "U.S. Demands," A5.

16. Lewis, "Asia."

17. Nakishima, "Indictment of PLA Hackers."

Chapter 10. Finding Meaning in the Expected Utility of International Cyber Conflict

1. Shakespeare, *Tragedy of Julius Caesar*, 3.2.288–290

2. Lindsay, "Stuxnet," 365–404. While Lindsay comes to the opposite conclusion in terms of the offense/defense problem, he readily admits this is due largely to the fact that he is basing

his assertion on a single case. Although he does not regard any other incidents rising to the same level as Stuxnet, he overasserts the distinction between cyber espionage and attack. Cyber espionage is largely about access and exploitation of that access. Although to date there is a lack of publicly acknowledged cases of espionage turned attack through access, there is sufficient public information available to indicate that adversaries have gained access to critical infrastructure in many different countries. Because of this evidence, the takeaway should not be that defense has the advantage, but rather that there is something else, be it strategic or tactical, that is constraining adversary behavior. The most likely constraint is not that critical infrastructure cannot be manipulated, but rather that it does constitute the option within the broader decision set with the greatest utility. Lindsay's article is, however, a powerful and compelling read.

3. Kahneman and Tversky, "Prospect Theory"; Liberman and Trope, "Role of Feasibility."

4. M. Friedman, "Methodology of Positive Economics," in Maki, *Methodology of Positive Economics*.

5. Bueno De Mesquita, *War Trap*; Bueno De Mesquita, "Expected Utility Theory."

6. "Update on Sony Investigation."

7. Viser, "Sony Was Wrong."

8. Lessig, *Code 2.0*, 5.

This page intentionally left blank

WORKS CITED

Abbate, Janet. *Inventing the Internet*. Cambridge: MIT Press, 2000.

Abrams, Marshall, and Joe Weiss. "Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia." August 2008. http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

Alberts, David S. *Understanding Information Age Warfare*. Washington, D.C.: CCRP Publication Series, 2001.

Albright, David, and Paul Brannan. "ISIS Imagery Brief: IAEA Inspectors and Iran Clash over Frequency of Inspections of Underground Facilities." Institute for Science and International Security, August 23, 2006. http://isis-online.org/uploads/isis-reports/documents/imagerybrief23august2006.pdf.

Alexander, Keith B. "Building a New Command in Cyberspace." *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 3–12.

Amoroso, Edward G. *Cyber Attacks: Protecting National Infrastructure*. Oxford: Butterworth-Heinemann, 2010.

Angstrom, Jan, and Isabelle Duyvesteyn. "Understanding Victory and Defeat in Contemporary War." New York: Routledge, 2007.

"Anonymous 'Takes Down' CIA Website." Aljazeera, February 11, 2012. http://www.aljazeera.com/news/americas/2012/02/201221020521840188 2.html.

Arquilla, John. "Cyberwar Is Already upon Us." *Foreign Policy*, February 27, 2012.

——— *Insurgents, Raiders, and Bandits: How Masters of Irregular Warfare Have Shaped Our World*. Chicago: Ivan R. Dee, 2011.

Arquilla, John, and David Ronfeldt. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, Calif.: Rand Corp., 1997.

Arrow, Kenneth J. "A Difficulty in the Concept of Social Welfare." *Journal of Political Economy* 58, no. 4 (1950): 328–346.

Axelrod, Robert, and Rumen Iliev. "Timing of Cyber Conflict." PNAS 111, no. 4 (2014): 1298–1303. January 13, 2014. http://www.pnas.org/content/111/4/1298.full.pdf+html.

Baldwin, David A., ed.

Neorealism and Neoliberalism: The Contemporary Debate. New York: Columbia University Press, 1993.

Barnes, Julian E., and Sioban Gorman. "U.S. Says Iran Hacked Navy Computers." *Wall Street Journal*, September 27, 2013. http://www.wsj.com/articles/SB10001424052702304526204579101602356751772.

Bearden, Milt, and James Risen. *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB*. New York: Random House, 2003.

Bedi, Rahul. "Mumbai Attacks: Indian Suit against Google Earth over Image Use by Terrorists." *Daily Telegraph*, December 9, 2008. http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html.

Benkler, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, Conn.: Yale University Press, 2006.

Berejikian, Jeffrey. "A Cognitive Theory of Deterrence." *Journal of Peace Research* 39, no. 2 (2002): 165–183.

Betz, David, and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. New York: Routledge, 2011.

Bilge, L., and T. Dumitras. "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World." Proceedings of the 2012 ACM Conference on Computer and Communications Security, Association for Computing Machinery, New York, 2012.

Billo, Charles, and Welton Chang. "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nations." Institute for Security Technology Studies at Dartmouth College, 2004. http://www.ists.dartmouth.edu/docs/execsum.pdf.

Black, Jeremy. *War and the World: Military Power and the Fate of Continents, 1450–2000*. New Haven, Conn.: Yale University Press, 1998.

Blainey, Geoffrey. *The Causes of War*. 3rd ed. New York: Free Press, 1988.

———. *The Main Enemy: The Inside Story of the CIA's Final Showdown with the KGB*. New York: Random House, 2003.

Brantly, Aaron. "The Changed Conversation about Surveillance Online." *NDItech*, National Democratic Institute for International Affairs, October 10, 2013. https://demworks.org/blog/2013/10/changed-conversation-about-surveillance-online.

———. "DDoS Mitigation 101." *NDItech*, National Democratic Institute for International Affairs, August 9, 2013. https://demworks.org/blog/2013/08/ddos-mitigation-101.

———. "Financing Terror Bit by Bit." *CTC Sentinel* 7, no. 10 (2014). https://www.ctc.usma.edu/v2/wp-content/uploads/2014/10/CTCSentinel-Vol7Iss10.pdf.

Brenner, Joe. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: Penguin Press, 2011.

Brenner, Susan W. "'At Light Speed': Attribution and Response to Cybercrime/Terrorism/Warfare." *Journal of Criminal Law and Criminology* 97, no. 2 (2007): 379–475.

Broad, William J., John Markoff, and David E. 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.

Bronk, Christopher. "Blown to Bits: China's War in Cyberspace, August–September 2020." *Strategic Studies Quarterly* 5, no. 1 (2011).

Bruner, Elgin M., and Manuel Suter. *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*. Zurich: Center for Security Studies, 2008.

Brynjolfsson, Erik, and Brian Kahin. "Understanding the Digital Economy: Data, Tools, and Research." Cambridge, Mass.: MIT Press, 2000.

Bueno de Mesquita, Bruce. "The Contribution of Expected Utility Theory to the Study of International Conflict." *Journal of Interdisciplinary History* 18, no. 4 (1988): 629–652.

———. "An Expected Utility Theory of International Conflict." *American Political Science Review* 74, no. 4 (1980): 917–931.

———. *The War Trap*. New Haven, Conn.: Yale University Press, 1981.

Campen, Alan D., ed. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax, Va.: AFCEA International Press, 1992.

Campen, Alan D., and Douglas H. Dearth. *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*. Fairfax, Va.: AFCEA International Press, 2000.

Carr, Jeffrey. *Cyber Warfare*. Sebastopol: O'Reilly Media, 2010.
Cerf, Vinton G. "The Day the Internet Age Began." *Nature* 461, no. 7268 (2009): 1202–1203.
Chickering, A. Lawrence. "Civil Society and Counterinsurgency." *Small Wars Journal* 6, no. 10 (2010).
Clark, Derek J., and Kai A. Konrad. "Asymmetric Conflict: Weakest Link against Best Shot." *Journal of Conflict Resolution* 51, no. 3 (2007): 457–469.
Clark, Wesley K., and Peter L. Levin. "Securing the Information Highway." *Foreign Affairs*, November/December (2009).
Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do about It*. New York: Ecco, 2010.
Clarridge, Duane R., and Digby Diehl. *A Spy for All Seasons: My Life in the CIA*. New York: Scribner, 1997.
Clausewitz, Carl von, Michael Howard, and Peter Paret. *On War*. Princeton, N.J.: Princeton University Press, 1976.
Clinton, Hillary Rodham. "Conference on Internet Freedom." Paper presented at the Conference on Internet Freedom, The Hague, Netherlands, 2011.
Conkey, Christopher, Elizabeth Williamson, and Cam Simpson. "Washington Metro Delayed Upgrades." *Wall Street Journal*, June 24, 2009.
Cooper, Jeffrey R. "Another View of the Revolution in Military Affairs." In *In Athena's Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla and David Ronfeldt, 99–140. Santa Monica, Calif.: Rand Corp., 1997.
Cornish, Paul, David Livingston, Dave Clemente, and Claire Yorke. "On Cyber Warfare." Chatham House, 2010. https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf.
Costigan, Sean S., and Jake Perry, eds. *Cyberspaces and Global Affairs*. Burlington, Vt.: Ashgate, 2012.
Cullather, Nick. "Bombing at the Speed of Thought: Intelligence in the Coming Age of Cyberwar." *Intelligence and National Security* 18, no. 4 (2006).
"A Cyber-Missile Aimed at Iran?" *Economist*, September 24, 2010. http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm.
"Cyber Power Index: Findings and Methodology." Economist Intelligence Unit, Booz Allen Hamilton, 2011. http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf.
"Cyber ShockWave—Simulation Report and Findings," Washington, D.C.: Bipartisan Policy Center, June 28, 2010.
Daugherty, William J. *Executive Secrets: Covert Action and the Presidency*. Lexington: University Press of Kentucky, 2004.
Dearth, Douglas H. "Operationalizing Information Operations: C2W . . . RIP." In Campen and Dearth, *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict*, edited by Alan D. Campen and Douglas H. Dearth, 97–109. Fairfax, Va.: AFCEA International Press, 2000.
"Defense Critical Infrastructure: GAO-08-373R." *GAO Reports*, April 2, 2008. http://www.gao.gov/assets/100/95438.pdf.
Demchak, Chris C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens: University of Georgia Press, 2011.
Dockrill, M. L., and David French. *Strategy and Intelligence: British Policy during the First World War*. London: Hambledon Press, 1996.

Downs, Anthony. *An Economic Theory of Democracy*. New York: Harper, 1957.

Doyle, Michael W., and Stephen Macedo. *Striking First: Preemption and Prevention in International Conflict*. Princeton, N.J.: Princeton University Press, 2008.

Drezner, Daniel W., and Henry Farrell. "Web of Influence." *Foreign Policy*, October 26, 2009. http://foreignpolicy.com/2009/10/26/web-of-influence/.

Einstein, Albert, and Alice Calaprice. *The New Quotable Einstein*. Princeton, N.J.: Princeton University Press, 2005.

Eriksson, Johnan, and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?" *International Political Science Review* 27, no. 3 (2006): 221–244.

"E-Stats, 2014 E-commerce Multi-sector Report." Washington, D.C.: U.S. Census Bureau, May 22, 2014.

"Europe: A Cyber-Riot; Estonia and Russia." *Economist*, May 12 2007.

Fair, C. Christine. "Drone Wars." *Foreign Policy*, May 28, 2010. http://foreignpolicy.com/2010/05/28/drone-wars-2/.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. "W32.Stuxnet Dossier." Symantec Security Response, February 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Farivar, Cyrus. "U.S. Indicts Suspected Anonymous Members for Leading 2010 'Operation Payback.'" *Ars Technica*, October 3, 2013. http://arstechnica.com/tech-policy/2013/10/us-indicts-suspected-anonymous-members-for-leading-2010-operation-payback/.

Faucon, Benoit. "New Sanctions Target Iran Oil Sales." *Wall Street Journal*, January 5, 2012. http://www.wsj.com/articles/SB10001424052970203471004577142262365335718.

Fearon, James D. "Rationalist Explanations for War." *International Organization* 49, no. 3 (1995): 379–414.

Finkle, Jim. "FBI Warns That Iran Hackers May Target U.S. Defense, Energy Firms." *Haaretz*, December 14, 2014. http://www.haaretz.com/news/world/1.631591.

Fishburn, Peter C. "Utility Theory." *Management Science* 14, no. 5 (1968).

Fisher, Richard D., Jr. "Cyber Warfare Challenges and the Increasing Use of American and European Dual-Use Technology for Military Purposes by the People's Republic of China (PRC)." Testimony for the Oversight and Investigations Subcommittee of the Foreign Affairs Committee of the United States House of Representatives. Hearing on "Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology." April 15, 2011.

Fishman, Charles. *The Wal-Mart Effect: How the World's Most Powerful Company Really Works—and How It's Transforming the American Economy*. New York: Penguin Press, 2006.

Friedman, Milton. "The Methodology of Positive Economics." In *The Methodology of Positive Economics: Reflections on the Milton Friedman Legacy*, edited by Uskali Maki, 3–44. Cambridge: Cambridge University Press, 2009.

Friedman, Thomas L. *The Lexus and the Olive Tree*. New York: Farrar, Straus and Giroux, 1999.

———. *The World Is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus and Giroux, 2005.

Fuhrmans, Vanessa. "Virus Attacks Siemens Plant-Control Systems." *Wall Street Journal*, July 22, 2010. http://www.wsj.com/articles/SB10001424052748703954804575381372165249074.

Fung, Brian. "How to Talk about Blowing Things Up in Cyberspace, according to the Military." *Washington Post*, July 23, 2014. http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/how-to-talk-about-blowing-things-up-in-cyberspace-according-to-the-military/.

"The Future of the Electric Grid: An Interdisciplinary MIT Study." Massachusetts Institute of Technology, December 5, 2011. http://web.mit.edu/mitei/research/studies/documents/electric-grid-2011/Electric_Grid_Full_Report.pdf.

Gartzke, Erik. "War Is in the Error Term." *International Organization* 53, no. 3 (1999): 567–587.

Geer, Daniel E. "Cybersecurity and National Policy." *Harvard National Security Journal* 1 (2010).

Geers, Kenneth. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review* 26, no. 3 (2010): 298–303.

Gibson, William. *Neuromancer*. New York: Ace Books, 1984.

Gill, Peter, Stephen Marrin, and Mark Phythian. *Intelligence Theory: Key Questions and Debates*. London: Routledge, 2009.

Goodman, Will. "Cyber Deterrence: Tougher in Theory than in Practice?" *Strategic Studies Quarterly*, Fall 2010: 102–135.

Gorman, Siobhan, and Julian E. Barnes. "Cyber Combat: Act of War." *Wall Street Journal*, May 31, 2011. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

Grafstein, Robert. "Rationality as Conditional Expected Utility Maximization." *Political Psychology* 161, no. 1 (1995).

Grauman, Brigid. "Cyber-Security: The Vexed Question of Global Rules." Brussels: Security and Defense Agenda, 2012. http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations." *Guardian*, June 11, 2013. http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Hafner, Katie. "Laurels for Giving the Internet Its Language." *New York Times*, February 16, 2005. http://www.nytimes.com/2005/02/16/technology/16internet.html.

Halpin, Edward F. *Cyberwar, Netwar and the Revolution in Military Affairs*. New York: Palgrave Macmillan, 2006.

Hart, Jeffrey A. "Information and Communications Technologies and Power." In Costigan and Perry, *Cyberspaces and Global Affairs*, 204–214.

Healey, Jason. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Arlington, Va.: Cyber Conflict Studies Association, 2013.

Henderson, Marlone D., Cheryl Wakslak, Kentaro Fujita, and John Rohrbach. "Construal Level Theory and Spatial Distance: Implications for Mental Representation, Judgment and Behavior." *Social Psychology* 42, no. 3 (2011): 165–173.

Herman, Michael. "Counter-Terrorism, Information Technology and Intelligence Change." *Intelligence and National Security* 18, no. 4 (2003): 40–58.

Horowitz, Michael, and Dan Reiter. "When Does Aerial Bombing Work? Quantitative Empirical Tests, 1917–1999," *Journal of Conflict Resolution* 45, no. 2 (2001): 147–173.

Hunker, Jeffrey, Bob Hutchinson, and Jonathan Margulies. "Role and Challenges for Sufficient Cyber-Attack Attribution." Dartmouth College: Institute for Information Infrastructure Protection, January 2008. http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf.

International Atomic Energy Agency. "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran." November 14, 2013. http://isis-online.org/uploads/isis-reports/documents/IAEA_Iran_Safeguards_Report_14Nov2013.pdf.

———. "Nuclear Verification." http://www.iaea.org/safeguards/symposium/2014/images/pdfs/verification.pdf.

"Iran Confirms Stuxnet Worm Halted Centrifuges." CBS News, November 29, 2010. http://www.cbsnews.com/news/iran-confirms-stuxnet-worm-halted-centrifuges/.

Jackson, Joab. "Google: 129 Million Different Books Have Been Published." *PCWorld*, August 6, 2010. http://www.pcworld.com/article/202803/google_129_million_different_books_have_been_published.html.

Janis, Irving L., and C. R. M. Productions. *Group Dynamics: Groupthink*. New York: McGraw-Hill Films, 1973.

Jefferson, Thomas. *The Writings of Thomas Jefferson*. 20 vols. Vol. 14 (1815). Ed. Andrew A. Lipscomb. Washington, D.C.: Thomas Jefferson Memorial Assn. of the United States, 1904–1905.

Jervis, Robert. "Political Implications of Loss Aversion." *Political Psychology* 13, no. 2 (1992): 187–204.

Jiga-Boy, Gabriela M., Anna E. Clarke, and Gun R. Semin. "Situating Construal Level: The Function of Abstractness and Concreteness in Social Contexts." *Social Cognition* 31, no. 2 (2013): 201–221.

Johnson, Loch K. *America's Secret Power: The CIA in a Democratic Society*. New York: Oxford University Press, 1989.

———. "On Drawing a Bright Line for Covert Operations." *American Journal of International Law* 86, no. 2 (1992): 284–309.

———. *Secret Agencies: U.S. Intelligence in a Hostile World*. New Haven, Conn.: Yale University Press, 1996.

———. *The Threat on the Horizon: An Inside Account of America's Search for Security after the Cold War*. New York: Oxford University Press, 2011.

Jones, Andy, Gerald L. Kovacich, and Perry G. Luzwick, *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton, Fla.: Auerbach, 2002.

Kahn, David. "The Intelligence Failure of Pearl Harbor." *Foreign Affairs*, December 1991.

Kahneman, Daniel, and Amos Tversky. "Prospect Theory: An Analysis of Decision under Risk." *Econometrica* 47, no. 2 (1979): 263–292.

Katyal, Neal Kumar. "Criminal Law in Cyberspace." *University of Pennsylvania Law Review* 149, no. 4 (2001): 1003–1114.

Kautalya, and L. N. Rangarajan. *The Arthashastra*. New Delhi: Penguin Books India, 1992.

Keeney, Michelle, and Eileen Kowalski. "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors." Washington, D.C.: United States Secret Service and Carnegie Mellon Software Engineering Institute, 2005. http://www.secretservice.gov/ntac/its_report_050516.pdf.

Kelly, Sanja, and Sarah Cook. "Freedom on the Net 2011: A Global Assessment of Internet and Digital Media." Washington, D.C.: Freedom House, 2011.

Keohane, Robert O. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, N.J.: Princeton University Press, 2005.

Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence*. 4th ed. Boston: Longman, 2012.

Krebs, Ronald R., and Aaron Rapport. "International Relations and the Psychology of Time Horizons." *International Studies Quarterly* 56, no. 3 (2012): 530–543.

Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (2011): 41–60.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, D.C.: National Defense University Press and Potomac Books, 2009.

Krekel, Bryan. "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation." Prepared for the US-China Economic and Security Review Commission. Mclean, Va.: Northrop Grumman, 2009.

Kshetri, Nir. "Information and Communications Technologies, Strategic Asymmetry and National Security." *Journal of Information Management* 11, no. 4 (2005): 563–580.

Landler, Mark, and John Markoff. "Digital Fears Emerge after Data Siege in Estonia." *New York Times*, May 29, 2007. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all.

Lardner, George, Jr. "U.S. Demands for Economic Intelligence Up Sharply, Gates Says." *Washington Post*, April 14, 1992, A5.

Lemos, Robert. "In Case of Cyber Attack: NATO Members Ready to Pledge Mutual Defense." *Ars Technica*, September 4, 2014. http://arstechnica.com/security/2014/09/in-case-of-cyberattack-nato-members-ready-to-pledge-mutual-defense/.

Lessig, Lawrence. *Code 2.0*. Cambridge, Mass.: Basic Books, 2006.

Levy, Jack S. "Misperception and the Causes of War: Theoretical Linkages and Analytical Problems." *World Politics* 36, no. 1 (1983): 76–99.

Lewis, James A. "Asia: The Cybersecurity Battleground: Statement before the House Foreign Affairs Committee, Subcommittee on Asia and the Pacific." July 23, 2013. Washington, D.C.: Center for Strategic and International Studies, 2013. http://csis.org/files/attachments/130723_jimlewis_testimony_v2.pdf.

———. "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Washington, D.C.: Center for Strategic and International Studies, 2009. http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

———. "Significant Cyber Incidents since 2006." Washington, D.C.: Center for Strategic and International Studies, 2014. http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf.

Lewis, James A., and Katrina Timlin. "Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization." Washington, D.C.: Center for Strategic and International Studies and United Nations Institute for Disarmament Research, 2011. http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf.

Liberman, Nira, and Yaacov Trope. "The Role of Feasibility and Desirability Considerations in Near and Distant Future Decisions: A Test of Temporal Construal Theory." *Journal of Personality and Social Psychology* 75, no. 1 (1998): 5–18.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, Calif.: RAND, 2009.

———. *What Is Information Warfare?* Washington, D.C.: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University. Washington, D.C.: Government Printing Office, 1995.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3. (2013): 365–404.

Lindsay, Jon R., and Lucas Kello. "Correspondence: A Cyber Disagreement." *International Security* 39, no. 2 (2014).

Lomsadz, Giorgi. "A Shovel Cuts Off Armenia's Internet." *Wall Street Journal*, April 8, 2011. http://www.wsj.com/articles/SB10001424052748704630004576249013084603344.

Lonsdale, David J. *The Nature of War in the Information Age: Clausewitzian Future*. New York: Frank Cass, 2004.

Lord, Kristin M. *The Perils and Promise of Global Transparency: Why the Information Revolution May Not Lead to Security, Democracy, or Peace*. Albany: State University of New York Press, 2006.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 5th ed. Washington, D.C.: CQ Press, 2011.

Lynn, William J., III. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September/October 2010.

Markoff, John. "Ideas & Trends: Blown to Bits; Cyberwarfare Breaks the Rules of Military." *New York Times*, October 17 1999.

Martin, Fredrick Thomas. *Top Secret Intranet: How U.S. Intelligence Built Intelink—the World's Largest, Most Secure Network*. Upper Saddle River, N.J.: Prentice Hall, 1999.

Mazanec, Brian M. "The Art of (Cyber) War." *Journal of International Security Affairs* 16, no. 2 (2009).

McCarthy, John A., with Chris Burrow, Maeve Dion, and Olivia Pacheco. "Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts." In Kramer, Starr, and Wentz, *Cyberpower and National Security*, 543–556.

McClure, Stuart. "Operation Cleaver." Cylance, 2014. http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.

McElroy, Damien, and Christopher Williams. "Flame: World's Most Complex Computer Virus Exposed." *Guardian*, May 28, 2012. http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html.

McGrath, Maggie. "Target Profit Falls 46% on Credit Card Breach and the Hits Could Keep On Coming." *Forbes Magazine*, February 26, 2014. http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W. W. Norton, 2001.

Metz, Cade. "Why Do We Call Them Internet Packets? His Name Was Donald Davies." *Wired*, September 10, 2012. http://www.wired.com/2012/09/donald-davies/.

Metz, Steven, and Douglas V. Johnson II. *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*. Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 2001.

Miard, Fabien. "Call for Power? Mobile Phones as Facilitators of Political Activism." In Costigan and Perry, *Cyberspaces and Global Affairs*, 119–144.

Minnick, Wendell. "Experts: Chinese Cyber Threat to U.S. Is Growing." *Defense News*, July 9, 2012. http://www.defensenews.com/article/20130709/DEFREG03/307090009/Experts-Chinese-Cyber-Threat-US-Growing.

Moravcsik, Andrew. "Taking Preferences Seriously: A Liberal Theory of International Politics." *International Organization* 51, no. 4 (1997): 513–553.

Nakishima, Ellen. "Indictment of PLA Hackers Is Part of Broad U.S. Strategy to Curb Chinese Cyberspying." *Washington Post*, May 22, 2014. http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html.

———. "List of Cyber-Weapons Developed by Pentagon to Streamline Computer Warfare." *Washington Post*, May 31, 2011.

———. "White House, NSA Weigh Cybersecurity, Personal Privacy." *Washington Post*, February 27, 2012.

National Security Act of 1947. 61 Stat. 495.

Nazario, Jose. "Politically Motivated Denial of Service Attacks." In *The Virtual Battlefield Perspectives on Cyber Warfare*, edited by Christian Czosseck and Kenneth Geers, 163–181. Amsterdam: Ios Press, 2009.

Nye, Joseph S., Jr. "Cyber Power." Cambridge, Mass.: Harvard Kennedy School of Government, Belfer Center for Science and International Affairs, 2010. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

———. *The Future of Power*. New York: Public Affairs, 2011.

Olson, James M. *Fair Play: The Moral Dilemmas of Spying*. Washington, D.C.: Potomac Books, 2006.

O'Mahony, Jennifer. "Stuxnet Worm 'Increased' Iran's Nuclear Potential." *Telegraph*, May 15, 2013. http://www.telegraph.co.uk/technology/news/10058546/Stuxnet-worm-increased-Irans-nuclear-potential.html.

Organski, A. F. K., and Jack Kugler. *The War Ledger*. Chicago: University of Chicago Press, 1980.

Owen, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, D.C.: National Academies Press, 2009.

Pape, Robert A. "The True Worth of Airpower." *Foreign Affairs*, March/April 2004.

"Paul Baran and the Origins of the Internet." RAND Corp., n.d. http://www.rand.org/about/history/baran.html.

Pillar, Paul R. *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform*. New York: Columbia University Press, 2011.

Pleming, Sue. "U.S. State Department Speaks to Twitter over Iran." Reuters, June 16, 2009. http://www.reuters.com/article/2009/06/16/us-iran-election-twitter-usa-idUSWBT01137420090616.

Potter, Richard, and Akihiro Nakao. "Mobitopolo: A Portable Infrastructure to Facilitate Flexible Deployment and Migration of Distributed Applications with Virtual Topologies." In *ACM SIGCOMM*. Barcelona: SIGCOMM, 2009.

"Presidential Directives and Executive Orders." Federation of American Scientists, n.d. http://www.fas.org/irp/offdocs/direct.htm.

Press, Daryl. "The Myth of Airpower: The Persian Gulf War and the Future of Airpower." *International Security* 26, no. 2 (2001): 5–44.

Quiggin, John. *Generalized Expected Utility Theory : The Rank-Dependent Model*. Boston: Kluwer Academic, 1993.

Rasmussen, Anders (NATO General Secretary). Question and answer session with the author following a talk at the United States Military Academy, October 8, 2014.

Reagan, Ronald. "Executive Order 12333—United States Intelligence Activities." Office of the President. Washington: U.S. Federal Register, 1981.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2011): 5–32.

———. *Cyber War Will Not Take Place*. London: Hurst, 2013.

———. "Think Again: Cyberwar." *Foreign Policy*, March/April 2012.

Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It." *Bloomberg Businessweek*, March 13, 2014. http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

Rohde, David. "The Obama Doctrine: How the President's Drone War Is Backfiring." *Foreign Policy*, February 27, 2012. http://foreignpolicy.com/2012/02/27/the-obama-doctrine/.

Rothkopf, David J. "Cyberpolitik: The Changing Nature of Power in the Information Age." *Journal of International Affairs* 51, no. 2 (1998).

Rumsfeld, Donald H. "DoD News Briefing—Secretary Rumsfeld and Gen. Myers." 2002. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636.

Russell, Bertrand. *An Outline of Intellectual Rubbish: A Hilarious Catalogue of Organized and Individual Stupidity*. Girard, Kans.: Haldeman-Julius, 1943.

Sabourin, Delphine, and Thomas Serval. "Electronization of Nasdaq: Will Market Makers Survive?" In *Internet and Digital Economics: Principles, Methods and Applications*, edited by Eric Brousseau and Nicolas Curien, 588–616. Cambridge: Cambridge University Press, 2006.

Samaan, Jean-Loup. "Cyber Command." *RUSI Journal* 155, no. 6 (2010).

Sanger, David E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown, 2012.

———. "Obama Order Sped Up Wave of Cyberattacks against Iran." *New York Times*, June 1, 2012. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.

Savio, Jessica. "Browsing History: A Heritage Site Is Being Set Up in Boelter Hall 3420, the Room the First Internet Message Originated In." *Daily Bruin*, April 1, 2011.

Schmitt, Michael N. *Tallinn Manual on the International Law Applicable to Cyber Warfare Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence*. Cambridge: Cambridge University Press, 2013.

Scott S. "We Are Anonymous, We Are Legion." *Yale Law and Technology*, November 9, 2009. http://www.yalelawtech.org/anonymity-online-identity/we-are-anonymous-we-are-legion/.

Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27, no. 1 (2008). http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7.

Shackley, Theodore, and Richard A. Finney. *Spymaster: My Life in the CIA*. Dulles, Va.: Potomac Books, 2005.

Shakarian, Paulo. "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, April 2011.

Shakespeare, William. *The Tragedy of Julius Caesar*, edited by Alvin B. Kernan. Rev. ed. The Yale Shakespeare. New Haven, Conn.: Yale University Press, 1959.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34, no. 1 (2010): 62–73.

Simon, Herbert A. "Human Nature in Politics: The Dialogue of Psychology with Political Science." *American Political Science Review* 79, no. 2 (1985): 293–304.

Simpson, J. A., and E. S. C. Weiner. *Oxford English Dictionary*. Oxford: Oxford University Press, 1989.

Singer, J. David. "Reconstructing the Correlates of War Dataset on Material Capabilities of States, 1816–1985." *International Interactions* 14, no. 2 (1987): 115–132.

Singer, J. David, Stuart Bremer, and John Stuckey. "Capability Distribution, Uncertainty, and Major Power War, 1820–1965." In *Peace, War, and Numbers*, edited by Bruce Russett. Beverly Hills, Calif.: Sage, 1972.

"SIPRI Military Expenditure Database." Stockholm: Stockholm International Peace Research Institute (SIPRI), 2012.

Skariachan, Dhanya, and Jim Finkle. "Target Shares Recover after Reassurance on Data Breach Impact." Reuters, February 26, 2014. http://www.reuters.com/article/2014/02/26/us-target-results-idUSBREA1P0WC20140226.

Skoudis, Edward. "Information Security Issues in Cyberspace." In Kramer, Starr, and Wentz, *Cyberpower and National Security*, 171–205.

Stein, Arthur. "Coordination and Collaboration: Regimes in an Anarchic World." In *Neorealism and Neoliberalism: The Contemporary Debate*, edited by David A. Baldwin, 29–59. New York: Columbia University Press, 1993.

Stokes, Mark A., Jenny Lin, and L. C. Russell Hsiao. "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure." Arlington, Va.: Project 2049 Institute, 2011.

Streich, Philip, and Jack Levy, "Time Horizons, Discounting, and Intertemporal Choice." *Journal of Conflict Resolution* 51, no. 2 (2007): 199–226.

Strezhnev, Anton, and Erik Voeten. "United Nations General Assembly Voting Data." 2013. http://hdl.handle.net/1902.1/12379 UNF:5:s7mORKL1ZZ6/P3AR5Fokkw==.

Strohm, Chris, and Wilber Del Quentin. "Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers." *Bloomberg News*, January 10, 2014.

"Target Data Breach Cost for Banks Tops $200M." NBC News, February 18, 2014. http://www.nbcnews.com/business/business-news/target-data-breach-cost-banks-tops-200m-n33156.

Thomas, Timothy L. "Cyber Mobilization: A Growing Counterinsurgency Campaign." Fort Leavenworth, Kans.: Department of Defense, 2006.

———. "Nation-State Cyber Strategies." In Kramer, Starr, and Wentz, *Cyberpower and National Security*, 465–488.

Thornton, Rod T. *Asymmetric Warfare: Threat and Response in the Twenty-First Century*. Cambridge Mass.: Polity Press, 2007.

Thucydides, Rex Warner, and M. I. Finley, *History of the Peloponnesian War*. Baltimore: Penguin Books, 1972.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *Guardian*, May 17, 2007. http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Treverton, Gregory F. *Covert Action: The Limits of Intervention in the Postwar World*. New York: Basic Books, 1987.

Trope, Yaacov, and Nira Liberman. "Construal-Level Theory of Psychological Distance." *Psychological Review* 117, no. 2 (2010): 440–463.

United Nations. Public Administration Network. "2012 Global E-Government Survey." New York: United Nations, 2012.

———. Educational, Scientific and Cultural Organization (UNESCO), Institute for Statistics. "United Nations Commodity Trade Statistics Database." New York: United Nations, 2012.

U.S. Cyber Command. "The Cyber Warfare Lexicon." Version 1.7.6. January 2009. https://publicintelligence.net/cyber-warfare-lexicon/.

U.S. Department of Defense. "Department of Defense Strategy for Operating in Cyberspace." Washington, D.C.: Department of Defense, 2011.

———. "Joint Doctrine for Command and Control Warfare (C2W)." Joint Chiefs of Staff. Washington, D.C.: Department of Defense, 1996.

———. "Joint Doctrine for Electronic Warfare Joint Publication 3-51." Washington, D.C.: Department of Defense, 2000.

———. "Joint Vision 2020." Washington, D.C.: U.S. Government Printing Office, 2000.

———. "The Military Power of the People's Republic of China: A Report to Congress." Washington, D.C.: Department of Defense, 2005. http://www.defense.gov/news/jul2005/d20050719china.pdf.

U.S. Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, D.C.: U.S. Dept. of Homeland Security, 2006.

———. *The National Strategy to Secure Cyberspace*. Washington, D.C.: U.S. Dept. of Homeland Security, 2003.

U.S. Dept. of Justice. "The President's Constitutional Authority to Conduct Military Operations against Terrorists and Nations Supporting Them." Opinion, 25 September 2001.

U.S. Federal Bureau of Investigation. "Update on Sony Investigation." National Press Releases, December 19, 2014. http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

U.S. Government Accountability Office. "Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented." GAO-13-187. Washington, D.C.: United States Government Printing Office, February 2013.

U.S. Office of the National Counterintelligence Executive. "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009–2011." Washington, D.C., 2011.

U.S. Office of the President. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." Washington, D.C., 2011.

U.S. Strategic Command. "The Cyber Warfare Lexicon: A Language to Support the Development, Testing, Planning and Employment of Cyber Weapons and Other Modern Warfare Capabilities." Version 1.7.6, January 5, 2009. https://info.publicintelligence.net/USSTRATCOM-CyberWarfareLexicon.pdf.

Van Evera, Stephen. *Causes of War*. Ithaca, N.Y.: Cornell University Press, 1999.

Viser, Matt. "Sony Was Wrong to Pull 'The Interview,' Obama Says." *Boston Globe*, December 19, 2014. http://www.bostonglobe.com/news/politics/2014/12/19/president-obama-says-sony-should-have-released-movie/kVdxy8WcsXVQZYAWoN8mRL/story.html.

Von Neumann, John, and Oskar Morgenstern. *Theory of Games and Economic Behavior*. Princeton, N.J.: Princeton University Press, 1944, 1953.

Waltz, Edward. *Information Warfare: Principles and Operations*. Boston: Artech House, 1998.

Waltz, Kenneth Neal. *Theory of International Politics*. Reading, Mass.: Addison-Wesley, 1979.

Warner, Michael. "Wanted: A Definition of "Intelligence." *Studies in Intelligence* 46, no. 3 (2002): 15–22.

"We Are Anonymous, We Are Legion." *Yale Law and Technology*, November 9, 2009. http://www.yalelawtech.org/anonymity-online-identity/we-are-anonymous-we-are-legion/.

Wendt, Alexander. "Constructing International Politics." *International Security* 20, no. 1 (1995): 71–81.

Wheeler, David A., and Gregory N. Larsen. "Techniques for Cyber Attack Attribution." Institute for Defense Analyses, November 11, 2013. http://www.ndia.org/divisions/divisions/cyber/documents/cyber-attack-attribution-wheeler.pdf.

Wheeler, Deborah L. "Information (without) Revolution? Ethnography and the Study of New Media-Enabled Change in the Middle East." In Costigan and Perry, *Cyberspaces and Global Affairs*, 155–172.

Williams, Brent T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Forces Quarterly*, 2nd Quarter 2014. http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/8461/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx.

Williams, Lawrence E., Randy Stein, and Laura Galguera. "The Distinct Affective Consequences of Psychological Distance and Construal Level." *Journal of Consumer Research* 40, no. 6 (2014): 1123–1138.

Williams, Phil, Timothy Shimeal, and Casey Dunlevy. "Intelligence Analysis for Internet Security." *Contemporary Security Policy* 23, no. 2 (2010): 1–38.

World Bank. World Development Indicators. http://data.worldbank.org/data-catalog/world-development-indicators.

"World Telecommunication/ICT Indicators Database Online." International Telecommunications Union, Switzerland 2011. http://www.itu.int/pub/D-IND-WTID.OL.

Worth, Robert F. "Iranian Supreme Leader Denies Nuclear Arms Push." *New York Times*, February 19, 2010. http://www.nytimes.com/2010/02/20/world/middleeast/20iran.html?_r=0.

Wortzel, Larry. "Assessing the Chinese Cyber Threat." *Defense Dossier* 4 (August 2012).

Zelizer, Julian E. *Arsenal of Democracy: The Politics of National Security—from World War II to the War on Terrorism*. New York: Basic Books, 2010.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown, 2014.

Zimet, Elihu, and Charles L. Barry. "Military Service Overview." In Kramer, Starr, and Wentz, *Cyberpower and National Security*, 285–308.

Ziobro, Paul, and Danny Yadron. "Target Now Says 70 Million People Hit in Data Breach." *Wall Street Journal*, January 10, 2014. http://online.wsj.com/articles/SB10001424052702303754404579312232546392464.

This page intentionally left blank

INDEX

f indicates figures; *t* indicates tables.

Abbottabad, covert operations in, 166
absolute value, 11–12
abstraction: spatial, 154; temporal, 153
Advanced Research Project Agency (ARPA), 2
affinity scores, 189
Afghanistan, covert action in, 56
Afghanistan War, 56
Ahmadinejad, Mahmoud, 14, 59
air battle, 100
air gap networks, 81
air power: in Gulf War, 94; in World War I, 90, 93
air war, 100
Alexander, Keith, 35, 102, 123
algorithms as basis of cyber, 103
alliances in cyberspace, 129
all-source intelligence, 102, 123
alternative cognitive approaches, 2
ambiguous deterrence, 113
Amoroso, Edward, 112, 124
Angstrom, Jan, 91
anonymity: as complex measure, 83–84; in cyberspace, 79–89, 128–129, 134–135, 158–159; defined, 79; expected utilities across incidents and, 139, 140–142, 141*t*; hazard function for, 86*t*, 86–87; importance of, 79, 80–84; layers of, 80; political action and, 84; positive utility of offensive cyber operations under, 163–164; probability function associated with, 151; probability of maintaining, by attack, 86*f*, 86–87; rational decision making and, 148; Stuxnet and, 83; value of, 84–86
anonymity-attribution problem, 23
Aristotle, 51
Armenia, 39
Army Cyber, Twitter account of, 28
Army Space and Strategic Defense Command, 36
ARPANET, 10; invention of, 7, 28
Arquilla, John, 109
Arrow, Kenneth, 18, 19; impossibility theorem of, 45, 126–127
ASCADA systems, 35
Aspin, Les, 53
asymmetry: conflict and, 25–26, 38; conventional, 37; in cyberspace, 37, 164; defined, 37–38; exploitation of, 38; in financial terms, 37; game theory in, 41; positive, 38; rational conflict and, 136
atomic bombs, 64
Atomic Energy Agency, 97
attacking states, concerns of, 79
attack recognition and attribution, 121*f*, 121–122
attribution: in cyberspace, 1, 10, 79–89; defined, 87
autocracies, unitary decision-making in, 15
Axelrod, Robert, 82

banks: central, 31; computerization of, 10
Baran, Paul, 2
bargaining range of war, 46, 47*f*, 91
Barry, Charles L., 39
battlefield: digital connections on, 104; intelligence preparation of, 110, 122*f*, 122–123
battlespace: attack recognition and attribution in, 121*f*, 121–122; defined, 110; differentiation between domestic and foreign, 111–112, 112*t*; importance of, 110; intelligence and cyber, 108–112; logical layer of, 110–111; physical layer of, 110; social layer of, 111; visualization of, 112
Benkler, Yochai, 28
Berejikian, Jeffrey, 151
Bernoulli, Daniel, 129

Betz, David, 133
bias: cognitive, 150, 156; importance for actors in cyberspace, 151; prospect theory and, 152
bilateral conflict, utility function for, 133, 135–136
bilateral policy range, 49*f*, 49–50, 56–57
Bilge, L., 82
Billo, Charles, 65
Bipartisan Policy Center, 69
Blainey, Geoffrey, 16
blending in, 38
blogosphere, 28
Boden, Vitek, 73
boundedness, theory of, 129
bounded rationality, 44, 46
Brenner, Jack, 33
Brenner, Joel, 88, 98, 105
Brenner, Susan, 80, 87
Bronk, Christopher, 95
Bueno de Mesquita, Bruce, 147; argument for bounded rationality of actors, 46; bilateral modeling of international conflict, 24; CINC scores of, 22, 77–78; coalition cohesiveness and, 127–128; on Cuban missile crisis, 19; defining of war by, 92, 93; as dominant decision-maker, 19–20; on expected utility, 1, 20, 21, 46–47, 48, 84–85, 100, 129–138, 163; monotonic decline in power and, 42; state alliances and, 23–24; on state conflict, 45; on Yule's Q tests, 149

Campen, Alan, 94, 110
capacity vulnerabilities, 39–40
Carr, Robert, 72
Census Bureau in tracking sales, 34
CENTCOM (U.S. Central Command), 23
Center for Strategic and International Studies, 72, 140, 162
central banks, 31
Central Intelligence Agency (CIA), 81, 123–124; provision of weapons to Afghanistan, 56
Chang, Welton, 65
Chickering, Lawrence, 28
China: anonymity and, 143; capability to conduct cyber warfare and cyber exploitation, 119; computer viruses in, 85, 95; development of cyber skills in, 40; foreign policy flap with, 88; People's Liberation Army in, 95–96, 118, 154–155; power disadvantage of, 157; risk-acceptant behavior in, 144
China-India attacks, 142–143
Clark, Derek, 118
Clark, Richard A., 58, 94, 109
Clarke, Anna E., 154
Clarridge, Duane, 53
Clausewitz, Carl von, 16–17, 34, 91, 98
Clinton, Hillary, 14
coalition cohesiveness, 127–128
coding, 2, 67–68; of complex scripts, 118
coding languages, 2–3
coercive action, forms of, 16
cognitive biases, 156; influence on human cognition, 150
cognitive processes in cyberspace, 150–156
combinatory attacks, 94–96
command and control warfare (C2W), 8–9, 36, 94, 95; as network centric, 105; origin of, 35
commands, 2
complex coding scripts, 118
complex interdependence, 28
Composite Index of National Capability (CINC) scores, 66–67; Bueno de Mesquita and, 22, 77–78; indexing equations for, 66
compromised hardware systems, 117*t*
computer emergency response teams (CERTs), development of, 119
computers: advances in, 7; importance of, 10
conflict, 90–100; as ambiguous, 92; asymmetric, 25–26; bilateral, 133, 135–136; combinatory attacks in, 94–96; conventional, 90; dynamics of, 90–100; initiation of, 120; language of, 90–93; motivation and rationality for, 45–50; negative utility for, 48; objective, scale, and tools of, 98–99; stand-alone, 97–98; war as ultimate form of, 91–92
constructivism, 10, 11
construct level theory (CLT), 152–156, 162
Consumer Bankers Association, 32
conventional asymmetry, 37
conventional conflict, decision to engage in, 90
conventional intelligence, 116, 118–119
conventional paradigm theorists, 16
coordination and collaboration, 48
Cornish, Paul, 82

Correlates of War (COW) project, 22, 92
counterterrorism intelligence analysis, 104
covert action, 43–62, 160; in Afghanistan (1980s), 56; anonymity as distinctive asset in, 80; categories of, 54; cyber as, 123–124; defined, 52; in Estonia (2007), 1, 56–58, 74, 83, 119, 132–133, 157; ladder for, 54, 55, 55*f*, 57; motivation and rationality for conflict, 45–50; Operation Cleaver and, 60–61; political utility and literature, 50–52; positive utility through, 54–56; setting basic assumptions, 44–45; as staple of state system, 43; Stuxnet and, 59–60, 83, 97–98, 115, 116, 118, 119–120, 133, 142, 148, 153–154; in Syria (2007), 58; threat of implementation of sanctions, 17; use of, for political utility, 52–56; utility of, 61–62
Credit Union National Association, 32
Crimean War, 6
criminal cyber exploits, 32
critical infrastructure, 117*t*
crypto-currencies, 105
Cuban missile crisis, 19
Cullather, Nick, 35, 104
cyber battle, 100
cyber battlespace, intelligence and, 108–112
cyber conflict: anonymity and, 157; applying expected utility theory of international, 138–141, 139*f*; decision-making and, 137
cyber-controlled instruments pertinent to national security, 5, 5*t*
cyber czar, 109–110
cyber defense, 15; importance of attribution to, 79
Cyber Defense Review, 28
cyber environment for defense (ICE-D), 106
cyber exploitation, 16, 117*t*; anonymity in, 81; defined, 15; historical accounting of attack types in, 116; network mapping and, 114–116; systemic vulnerabilities and, 116
cyber hostilities, 39
cyber literature, defensive orientation of, 103
cyber operations, 52, 133; defensive, 88–89
cyberpolitik, as realpolitik, 27
cyber power, 22–23; categories of, 63; conceptualizing, 63, 76–78, 77*t*; defined, 64–65; equation for, 76; indexing equation for, 72–73; theoretical aspects of, 72
Cyber Power Index, 65–66
Cyber ShockWave, 69, 70
cyberspace, 16, 22, 32; act of war in, 113; alliances in, 129; anonymity in, 79–89, 128–129, 134–135, 158–159; asymmetry in, 25–26, 37; attribution in, 1, 10, 79–89; civilian aspects of, 1, 101; cognitive processes and decision-making in, 150–156; coining of, as term, 2; computers as basic unit of, 2; concern for science facts, 166; construction of power in, 164; conventional tools and, 98–100, 99*f*; as covert action, 123–124; decision-making model for, 1, 85, 158–161; defined, 1, 4–6, 15; dependence on, 4; deterrence in, 87–88; as domain, 7, 12, 93; economy and, 33–34; effect of weather on, 36; as force multiplier, 95–96; force size and, 118; as fragile, 4; history of, 2, 71–72; impact of intelligence preparation on battlefield on, 122*f*, 122–123; importance of, 1, 3, 4; informational-sharing purposes of, 96; infrastructure and, 26, 27*f*; intelligence in, 101–124; international relations and, 10–12, 16; in joint doctrine publications, 112–114; lexicon of, 15*t*; major problem with, 108; as man-made, 1, 101–102, 164; military capabilities in, 1, 101; national security and, 1, 5*t*, 9, 12, 26–27, 37, 166; open source analysis of capabilities, 118; operations in, 158; physics and algorithms as basis of, 103; as porous domain, 73; presidential directives, decisions, and executive orders pertaining to, 8, 8*t*; rank ordering of nations in, 67; rational choice approach to using, 125–149; references to, 9; response mechanism to, 88; security studies on, 12; states as rational actors in, 125, 157; theoretical limits of, 66–67; uniqueness of, 12; value of, 3; vulnerabilities of, 73–76
cyber war, 38, 100; capability in, 15; defined, 15; lexicon of, 15; unit size in, 67–68
Cyberwar 3.0, 110
"Cyber Warfare" (Billo and Chang), 65
cyber weapon systems, 23, 64, 98; decision-making processes for use of, 103; defined, 15; destructive power of, 158
Cylance, 60–61, 153

Dartmouth Report on Cyber Warfare, 72
data, 161; breach of, at Target Corporation, 32; constraints on, 167; limitations of, 161–162; longitudinal availability of, 161
Davies, Donald, 2
Dearth, Douglas, 34, 110
decision-making in cyberspace, 1, 85, 150–156, 158–161
decision-making model: construction across capabilities measures, 90; neoliberalism and, 11; rational, 1, 11; unitary, 15, 21
Defense, U.S. Department of: on cyber attacks, 100; establishment of USCYBERCOM by, 35; facilitation of network protection, 106; impact of information revolution on, 8; Joint Doctrine for Command and Control Warfare, 113; "Joint Vision 2020" of, 25, 101; as networked environment, 68; penetration of networks on, 25; strategy for operating in cyberspace, 113
Defense Advanced Research Project Agency, 81; invention of ARPANET by, 7
Defense Information Systems Agency, 36
defensive cyber operations (DCOs), 88–89
defensive cyber operations–internal defensive measures teams (DCO-IDM), 106, 107
defensive cyber operations–response action teams (DCO-RA), 106, 107
demonstrated capabilities, 63
denial of service attack (DOS), 117*t*
deterrence, 87–88
digital espionage, 33
digital power, 63–78
digital tools, terrorist use of, 105
diplomacy, transparency in, 30
discounted utility, 152
distributed denial-of-service (DDoS) attacks, 57, 81–82, 83, 117*t*, 156; on Estonia, 74
DoD information network operations teams (DoDIN Ops), 106; mentality of, 107
dominant battlespace awareness (DBA), 108, 112*t*
dominant battlespace knowledge (DBK), 108, 112*t*
Douhet, Giulio, 90, 93
Downs, Anthony, 51
Drezner, Daniel, 28
dual covert-overt attack, 58
Dumitras, T., 82
Dunlevy, Casey, 105, 108
Duyvesteyn, Isabelle, 91

E-commerce, 34
economic covert action, 54
economic pillar in national security, 25, 31–34
economics, global, 31
economic sanctions, 14, 83
economic security, 11
Economist Intelligence Unit's (EIU), 68; "Cyber Power Index," 65–66
economy, ties to cyberspace, 33–34
Einstein, Albert, 43
electric grid, 35
electricity, military and civilian reliance on, 35
electromagnetic spectrum, 5
electronic data interchanges (EDIs), 31
electronics, 5
environmental pillar in national security, 25, 36–42
environmental security, importance of, 36–42
environmental vulnerabilities, 39–40
equipment disruption, 117*t*
espionage, 53
Estonia: Cyber Power Index and, 66; 2007 cyber attacks against, 1, 56–58, 74, 83, 119, 132–133, 157
European telegraph lines, extension of, 6
ex-ante settlement, 50
Executive Order 12333, 115, 123
Executive Order 13636, 32, 105, 106, 165
expected utility, 160; applying theory of, 138–141, 139*f*; Bueno de Mesquita on, 1, 20, 21, 46–47, 48, 84–85, 100, 129–138, 163; finding meaning in, 157–167; implications of, 162–167; of states across incidents, 140–143, 141*t*
ex-post inefficiencies, 45

Farrell, Henry, 28
Fearon, James, 43, 44, 45, 46–47, 48, 50, 53, 58, 62, 91, 127
Federal Bureau of Investigation (FBI), 81, 165
financial terms, asymmetry in, 37
firewalls, 81
firmware, 3
Fishburn, Peter, 51, 129

Flame, 142
Fleet Cyber Command of the U.S. Tenth Navy, 164
"fog of war," 34
food security, 11
force multiplier, cyber as, 95–96
Foreign Intelligence Surveillance Act, 115
Friedman, Milton, 162
Friedman, Thomas, 31
full-spectrum dominance, U.S. strategy of, 12
fusion centers, creation of, 104

game theory: impossibility theorem and, 20; logic of symmetry using, 41
Gartzke, Erik, 92
Gates, Robert, 155
Geers. Kenneth, 89
Georgia, 39; cyber operations against, 157; Cyber Power Index and, 66; hostilities between Russia and, 39, 95, 96; Russian Federation's cyber attacks on, 71
geospatial intelligence (GEOINT), 103, 104*t*
Germany, cyber power score of, 139
global economics, 31
globalization, 31
Goodman, Will, 40
Google Earth, 105
Government Accountability Office (GAO), report on national strategy, roles, and responsibilities, 70
Grafstein, Robert, 52
green uprisings, 14
ground battle, 100
ground war, 100
Guardian Project, tools from, 30
Gulf War, 8–9, 35, 74, 94; air power used in, 94
Gutenberg press, 7

hard power, 64; applications of, 14; defining, 13–14; defining components of digital, 65–73, 73*t*; difference between soft power and, 13; objectives of, 13–14
Hart, Jeffrey, 63
Hathaway, Melissa, 109
hazard model, 85–87; anonymity and, 86*t*, 86–87
Henderson, Malone D., 153–154
Herman, Michael, 104
HEU, Iran's movement toward, 60
historical variables as imperfect, 71–72
Hitler, Adolf, 44
Hobbes, Thomas, 64
Homeland Security, U.S. Department of, 165; informational-sharing activities in, 33
Hong Kong, 29
Horowitz, Michael, 93, 97
hostile covert action, 18
hostile overt bargaining, 18
Hsiao, L. C. Russell, 118
human cognition, influence of cognitive biases on, 150
human intelligence (HUMINT), 103, 104*t*, 108, 119–121
human vulnerabilities, 40
Hunter Watertech, 73–74
Hussein, Saddam, 74

ICANN, 11
Illiev, Rumen, 82
impossibility theorem, 18, 19, 126–127; game theory and, 20
India, cyber power score of, 138–139
industrial applications, 68–69
industrial control systems (ICS), 3, 36, 61
information: defined, 5; diffusion of, 28; use of cyber for sharing, 96; value of, 7, 9
information communications technology (ICT), 4; advances in, 6, 7; economics and, 31–34; effect on political and social movements, 30; in facilitation of information revolution, 28; importance for civil development, 28; mitigation of stovepipes and, 104; in national security, 30; public-private collaborations in, 118–119; reliance on modern militaries, 34–35; role of, 104; value associated with, 9
Intelink, creation of, 35
intelligence: all-source, 102, 123; collection of, 103–104, 104*t*; conventional, 116, 118–119; cyber battlespace and, 108–112; in cyberspace, 101–124; defining, 102–108; geospatial, 103, 104*t*; in honing vulnerability, 73; human, 103, 104*t*, 108, 119–121; measurement and signatures, 103, 104*t*; open source, 103, 104*t*, 108; signals, 103, 104*t*, 108

intelligence collection types (INTs), value of, 102
intelligence cycle, 108–109; as linear, 109
intelligence preparation of the battlefield (IPB), 110; impact on cyber, 122*f*, 122–123
Intelligence Reform and Terrorism Prevention Act (2004), 104
Intellipedia, creation of, 35
interdependence, 11–12
International Atomic Energy Agency (IAEA), 59
International CIIP Handbook, 37
international conflict, rational initiation of, 47
international politics: anonymity and, 79; as positive sum game, 17
international relations: areas of study in, 16; cyber and, 10–12, 16; literature in, 28; power in, 63–65
International Telecommunications Union (ITU), 11, 149; data on Internet penetration, 41; measurement of digital dependence and, 75*f*, 75–76; measurement of Internet penetration, 42
Internet: defining, 2; firewalls and, 81; origin of, 81; penetration of, 42; users of, 7–8, 41*f*, 75*f*
Internet kill switch, 23
Internet service provider (ISP), 4
Internet Society, 11
interstate communications and perceptions, social distance in, 154–155
Iran: Ahmadinejad as president of, 14, 59; Cyber Power Index and, 66; Green uprisings in, 14; movement toward HEU, 60; nuclear program in, 14, 59, 98, 154; sanctions against, 14; use of Twitter in, 14, 29
Iron Curtain, 10
Israel: attack on Syrian nuclear facilities, 71, 133, 142; Cyber Power Index and, 66; multiplier debate and, 96; use of cyber beams, 58

Janis, Irving, 52
Jefferson, Thomas, 63
Jervis, Robert, 150
Jiga-Boy, Gabriela M., 154
Johnson, Douglas V., 37–38
Johnson, Loch, 52, 53–54, 102
joint doctrine publications, cyber domain in, 112–114
JP 3-51 electronic warfare-planning model, 120
jurisdictional authority, need for, in cyber attack, 70
Justice, U.S. Department of: on undeclared conflict, 92; on wars in Clausewitzian sense, 98

Kahneman, Daniel, 52, 150–151, 162
Kautilya, 43
Keohane, Robert O., 16, 28, 34; *Power and Independence* (with Nye), 10
Kim Jong-un, 164
kinetic warfare operations, 96
Kissinger, Henry, 52–53
Klimburg, Alexander, 119
Knake, Robert K., 58
Konrad, Kai, 118
Kramer, Franklin D., 4, 64, 77, 133
Krebs, Ronald R., 152
Kshetri, Nir, 38–39
Kuehl, Dan, 4, 5, 6
Kugler, Jack, 136

languages, programming, 2
Larson, Gregory N., 87
legal variables, 69–70
Lessig, Lawrence, 166
Levy, Jack S., 16
Liberman, Nira, 153, 162
Lin, Jenny, 118
Lindsay, Jon R., 157
literature: defensive orientation of cyber, 103; in international relations, 28; political utility and, 50–52
Lord, Kristen, 30
Lynn, William, 35

Machiavelli, 102
MAC OS X Yosemite, 111
"Maginot Line" strategy, 106
malicious software, 59
Manning, Bradley (now Chelsea), diplomatic leaks by, 30, 120
market-based approach toward risk mitigation, 32

Marrin, Stephen, 108–109
mathematics, security measures and, 103
McCarthy, John, 31
Mearsheimer, John J., 11, 16, 45
measurement and signatures intelligence (MASINT), 103, 104*t*
Mercosor, 17
Metz, Steven, 37–38
Miard, Fabien, 28
Middle East, revolutions across, 29
military: capabilities of, as closely guarded secret, 116; in covert action, 54; as pillar in national security, 25, 34–36; reliance on informational communications technologies, 34–35; security as coordinated effort, 36
military-industrial complex, connectedness in, 35
Mitchell, Billy, 93
modified economist intelligence unit component values, 169–187
monotonic loss of utility, 153
Moravcisk, Andrew, 16
Morgenstern, Oskar, 18, 20, 51, 129
multinational corporations, rise of, 10
Mumbai terrorist attacks (2008), 105
mutual defense, NATO pledge for, 113

Napoleonic era, military in, 64
Natanz: enrichment uranium production at, 153; Stuxnet attacks on, 133, 153–154
national digital dependence, 63
National Infrastructure Protection Plan, 37
national security: cyberspace and, 1, 5*t*, 9, 12, 26–27, 37, 166; economic pillar in, 25, 31–34; examples of cyber-controlled instruments pertinent to, 5, 5*t*; information communications technology in, 30; military pillar in, 25, 34–36; modern structure of, 27, 27*f*; pillars of, 25; political and social pillar in, 25, 27–30
National Security Act, 52
National Strategy to Secure Cyberspace, The, 80, 105
NATO, 58; Article 5 response, 57, 58, 113; Cooperative Cyber Defense Centre of Excellence of, 58; pledge for mutual defense, 113
Nazario, Jose, 39
negative asymmetries, 38
negative utility for conflict, 48
neoliberalism, 10, 11, 28, 44, 50
neorealism, 10, 11, 44
network-centric warfare, 9, 104
networked controls, 26
network mapping, 114–116
Neumann, John Von, 18, 51
9/11, terrorism prior to, 109
Nixon, Richard M., 53
NMCI (Navy Marine Corps Intranet), 60–61
nondemocratic societies, unitary decision-making in, 15
nonhostile overt bargaining, 18
non-interdependence, realist world of, 10
nonmonotonic decline in expected utility, 152
Non-Proliferation Treaty (NPT), 59
North Africa, revolutions across, 29
North Korea: cyber attack against Sony Pictures Entertainment, 164–165; offensive cyber unit in, 74
nuclear security, 11
Nye, Joseph, 13, 16, 28, 34, 64, 65, 133; *Power and Independence* (with Keohane), 10

Obama, Barack, 21, 52, 59, 83
offensive cyber operations (OCOs), 22, 107, 160, 161; under anonymity, 87, 163–164; as form of covert action, 43; initiation of, 50
Olson, James M., 53
Olympic Games, 157; Obama's authorization of, 59
open source cryptography, 105
open source intelligence (OSINT), 103, 104*t*, 108
open source research, 105
Operation Cleaver, 60–61, 153
Operation Payback (2010), 81–82
Organski, A. F. K., 136
overt diplomacy, gap between overt war and, 62
Owens, David, 79

Pakistan, covert drone strikes in, 52
Pape, Robert, 93
Pearl Harbor, bombing of, 7
Pelé, 74–75

Pentagon, terrorist attack on, 109
Persian Gulf War, 93
personally identifiable information, 61
physics as basis of cyber, 103
PLA (People's Liberation Army), 95–96, 118, 154–155
policy affinity, 140
policy platforms, 114
policy process, categories of, 18
policy range, bilateral, 49*f*, 49–50, 56–57
political action, anonymity and, 84
political acts, anonymity and, 79
political covert action, 54
political pillar in national security, 25, 27–30
political utility, 43, 160; literature and, 50–52; use of covert action for, 52–56
politicking, 17
politics, 17; power in, 63–64; as term, 51
positive expected utility, 45
positive utility through covert action, 54–56
power, 63; as ambiguous concept, 63; conventional studies on, 64; hard, 13–14, 64, 65–73, 73*t*; in international relations, 64–65; "push" applications of, 65; in rational choice modeling of war, 64; soft, 13–14, 64; in traditional sense, 63
Power and Independence (Keohane and Nye), 10
power scores: comparison of, 84; components of, 168; by country, 76–77, 77*t*; defined, 138–139, 139*f*
power stations, computerization of, 10
preference ordering, 18
Press, Daryl, 94
probability function, association with anonymity, 151
programmable logic controllers (PLCs), 26, 115
programming languages, 2
propaganda, 54, 117*t*; web, 87
prospect theory, 150–152, 162; biases associated with, 152
proximity, U.S. cyber community and, 107
psychological distance, 153
public-private ICT collaborations, 118–119
public square, fundamental change in, 28, 29
push mechanism of intelligence community, 109

quiet option, 52
Quiggin, John, 129

radio triangulation, 6–7
rank dependent expected utility (RDEU) model, 129
Rapport, Aaron, 152
Rasmussen, Anders, 113
rational actor model, 2
rational choice approach, 1, 18, 125–149, 162; data in context, 148–149; to decision making, 1, 157; examining propositions in, 143–147, 144*t*, 145*t*, 146*ft*; expected utility of states across incidents in, 140–143, 141*t*; expected utility theory of international cyber conflict in, 138–140, 139*f*; logic of, 12–24; neoliberalism and, 11; power in, 64; rationality in, 125, 126–127; states in, 12–24, 157; uncertainty and risk in, 127–129; utility theory of (cyber) conflict in, 129–139
rationality, 126–127; bounded, 44, 46; fallibilities of, 44; prediction of, 125
realism, 11
Redstone Arsenal, 36
regulatory variables, 69–70
Reiter, Dan, 93, 97
resource vulnerabilities, 39–40
revolution in military affairs (RMA), 9
Rid, Thomas, 84, 94
risk-acceptant actors, 129
risk-averse actors, 129
risks: market-based approach toward mitigating, 32; in rational choice approach, 127–129
robotics, 26
Rogers, Michael, 123
Ronfeldt, David, 109
ROTC, 165
Rothkopf, David, 27
Rumsfeld, Donald, 106
Russell, Bertrand, 125
Russia: cyber attack as act of, 114; denial of participation in cyber attacks against Estonia, 119; hostilities between Georgia and, 39, 95, 96
Russia-Georgia war of 2008, 142, 156
Russian Federation, 132; cyber attacks against Estonia and, 57–58; cyber attacks on Georgia, 71

Samaan, Jean-Loup, 9
sanctioning, 14, 83

Sanger, David, 59
science, security measures and, 103
Second Army–U.S. Army Cyber Command, 164
semaphore, 6
Semin, Gun R., 154
service academies, 165
Shackley, Theodore, 53
Shakespeare, William, 157, 159
Sharma, Amit, 97, 98
Shimeal, Timothy, 105, 108
signals intelligence (SIGINT), 103, 104*t*, 108
silent option, 52
Simon, Herbert, 44
Singer, David, 22
Snowden, Edward, 9, 103, 120
social distance, 154–156; U.S.-China relationship as example of, 155
social pillar in national security, 25, 27–30
social scientific analysis, power in, 64
soft power, 64; defining, 13–14; difference between hard power and, 13; objectives of, 13–14
software, 3; malicious, 59
Sony Pictures Entertainment (SPE), cyber attack against, 164–165
Soviet Union: Afghanistan War and, 56; pipeline management software stolen by, 98. *See also* Russia; Russian Federation
space war, 100
spatial abstractions, 154
spatial distance, 153–154
stand-alone conflict, 97–98
Starr, Stuart H., 4, 64, 77, 133
states: concerns of attacking, 79; rational choice modeling and, 12–24, 157; role of power in influencing actions, 63; understanding policy positions of, 14*f*, 14–15
Stein, Arthur, 48
Stevens, Tim, 133
Stokes, Mark A., 118
stovepipes, mitigation of, 104
strategic ambiguity, 113
Strezhnev, Anton, 130
Stuxnet, 142, 148; anonymity and, 83; distribution of, 119–120; enrichment of uranium by Iran and, 59–60; exposure of zero-day vulnerabilities, 116, 118; forensic analysis of, 115; intended objective of, 97–98; on Natanz, 133, 153–154
Sun Tzu, 43, 51, 101, 102
supervisory control and data acquisition (SCADA) systems, 26, 61
surface-to-air missiles (SAMs), 94–95
SVR, 57
Symantec, 59
Syria: covert actions against, 56–58; Cyber Power Index and, 66; Israeli cyber attacks against, 71, 87, 133, 142
systemic vulnerabilities, 116

tactics, techniques, and procedures (TTP), 118; ability to leverage cyberspace for soft power gain, 13
Tails, 29
Tallinn, 119
Tallinn Manual on the International Law Applicable to Cyber Warfare, 114
Target Corporation, data breach at, 32
TCP/IP (Transmission Control Protocol/Internet Protocol), 2; invention of, 28
technological infrastructure, 68–69
telegraph lines, problems with, 6
temporal abstraction, 153
terrorism, 105; digital tools in, 105; in Mumbai, 105; prior to 9/11, 109
theoretical capabilities, 63
Theory of International Politics (K. Waltz), 10
third option, 52
Thornton, Rod, 39
threat spectrum capabilities, 116, 117*t*
Thucydides, 64
Titan Rain, 38, 80
Tor network, 29–30
Track II diplomacy, 44, 52
Tragedy of Julius Caesar (Shakespeare), 157, 159
transparency in diplomacy, 30
Treasury, U.S. Department of, 165
Treverton, Gregory, 52
Trope, Yaacov, 153, 162
Truman, Harry, 15
t-tests in testing propositions, 161
Tversky, Amos, 52, 150–151, 162
Twenty-Fourth Air Force–Air Forces Cyber, 164
Twitter, 14, 29

Ukraine, 29
uncertainty in rational choice approach, 127–129
unitary decision making: in autocracies, 15; basis for decisions of, 21
United Nations, 17; Institute for Disarmament Research, Security and Defense Agenda, 71–72; voting affinity scores of, 149
United States: arms race with Russia and origin of cyberspace, 2; cyber attack as act of, 114; cyber power score of, 138–139; dependency of military and intelligence communities on data exchange and maintenance, 9; proximity and, 107; War on Terror in, 37
U.S.-China Economic and Security Review Commission, 119
U.S. Cyber Command (USCYBERCOM), 5–6, 15, 64, 102; creation of, 34; in managing network defense, 35
U.S. Cyber United, 67
U.S. Logistics Command, 80
U.S. Strategic Command (STRATCOM), 15, 124
utility, 18; of covert action, 61–62; discounted, 152; economic terminology associated with, 51; monotonic loss of, 153; political, 43, 50–52; positive expected, 45
utility modeling, 18, 20
utility theory, 18; Bueno de Mesquita on, 129–138

Van Evera, Stephen, 16
VirusBlokAda, 59
virus code in China, 85, 95
Voeten, Erik, 130
Von Neumann, John, 20, 129
vulnerabilities: capacity, 39–40; environmental, 39–40; human, 40; multiple causes of, 39; origination of, 39; resource, 39–40; zero-day, 38, 111, 116, 118

Walmart, inventory management system at, 33
Waltz, Edward, 108, 110, 112, 122
Waltz, Kenneth, 10, 16, 45; *Theory of International Politics*, 10
war: bargaining range of, 46, 47*f*, 91; Chinese capability to conduct, 119; Clausewitz on, 98; command and control, 8–9, 94, 95; cyber, 15, 38, 67–68, 93, 100, 113; fog of, 34; gap between overt diplomacy and, 62; ground, 100; kinetic operations, 96; logic behind causes of, 45; network-centric, 9, 104; overt, 62; physical and kinetic concept of, 91; rational choice modeling of, 12–24, 18, 64, 127; space, 100; as ultimate form of conflict, 91–92. *See also* Gulf War; World War I; World War II
Warner, Michael, 102, 103, 123, 124
weapons: covert deployment of, 56; cyber, 15, 23, 56, 64, 98, 103, 158
weather, effect on cyber domain, 36
Weber, Max, 64
web of influence, evolution of, 28
web propaganda, 87
web vandalism, 117*t*
Wendt, Alexander, 11
Wentz, Larry K., 4, 64, 77, 133
Wheeler, Deborah L., 29, 87
Wiki-leaks, 9, 30
Williams, Phil, 105, 108
Wilson's War (film), 56
World Bank, 34
World Trade Center, terrorist attack on, 109
World Trade Organization, 17
World War I: air power during, 90, 93; radio transmission during, 6
World War II: blitz on London in, 98; bombing of Pearl Harbor in, 7; Hitler in, 44; instigation of hostilities in, 21; radar in, 6–7; societal mobilization for victory in, 93; strategic bombing in, 93
World Wide Web, 10
World Wide Web Consortium, 11

Yule's Q tests, 149

Zelizer, Julian E., 91
zero-day exploits, 39
zero-day vulnerabilities, 111; manipulation of, 38; Stuxnet and, 116–118
zero-sum bargaining, 17
zero-sum interactions, 48
Zimet, Elihu, 39