INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES

Information Warfare

2nd Edition revised and Updated

Daniel Ventre



ISTE

WILEY

Information Warfare

Revised and Updated 2nd Edition

Information Warfare

Daniel Ventre

ISTE

WILEY

First published 2016 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form or by any means, with the prior permission in writing of the publishers, or in the case of reprographic reproduction in accordance with the terms and licenses issued by the CLA. Enquiries concerning reproduction outside these terms should be sent to the publishers at the undermentioned address:

ISTE Ltd
27-37 St George's Road
London SW19 4EU
UK

www.iste.co.uk

John Wiley & Sons, Inc.
111 River Street
Hoboken, NJ 07030
USA

www.wiley.com

© ISTE Ltd 2016
The rights of Daniel Ventre to be identified as the author of this work have been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

Library of Congress Control Number: 2015959669

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-660-0

Contents

Introduction ix

Chapter 1. The United States 1

1.1. Information warfare in the 1990s. 1
1.1.1. Points of view from security experts 1
1.1.2. US Air Force Doctrine: AFDD 2-5 (1998) 7
1.1.3. The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (1998) 10
1.1.4. Components of information warfare 14
1.2. Information warfare in the 2000s. 23
1.2.1. Dictionary of the Department of Defense 23
1.2.2. US Air Force: AFDD 2-5 (2005) and AFPD 10-7 (2006) 24
1.2.3. The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (2006) 26
1.3. Information warfare in the 2010s. 28
1.4. Important concepts and reflections. 43
1.4.1. Information operations 44
1.4.2. Information superiority 51
1.4.3. The “value” of information. 62
1.4.4. Information system 65
1.4.5. Command and control warfare: C2W. 66
1.4.6. Effect-based operations (EBOs) 68
1.4.7. The OODA loop 69
1.4.8. RMA 70

1.4.9. C4ISR 72
1.4.10. Network centric warfare (NCW) 73
1.4.11. ISR: intelligence, surveillance, reconnaissance. 74
1.4.12. Cyberwar 75
1.4.13. Netwar. 89

Chapter 2. China 91

2.1. Significant publications 91
2.2. Strategic and doctrinal thinking about information warfare. Genesis 96
2.2.1. General Wang Pufeng: one of the pioneers 97
2.2.2. Wang Baocun and Li Fei 100
2.2.3. Wei Jincheng 104
2.2.4. Colonels Qiao Liang and Wang Xiangsui: unrestricted warfare 105
2.2.5. General Dai Qingmin and Wang Baocun 111
2.2.6. General Niu Li, Colonel Li Jiangzhou and Major Xu Dehui. 114
2.2.7. 2004 White Paper on national defense 115
2.3. Recent policies and strategies on information and cyber security 117
2.3.1. The Science of Military Strategy 2013 118
2.3.2. Defense White Paper 2013 118
2.3.3 Sino-Russian cybersecurity agreement 2015 119
2.3.4. *PLA Daily* editorial on 20 May 2015 121
2.3.5. Defense White Paper of 26 May 2015. 122
2.3.6. The national cybersecurity bill of July 2015 125
2.4. Reflections 125
2.4.1. The American perspective on Chinese information warfare, modernization and informatization of the PLA 125
2.4.2. Evolution of analyses and discourse about Chinese strategy 163
2.4.3. China as a “victim” 172
2.4.4. The strategy of active defense 173

Chapter 3. Russia 177

3.1. Military doctrines and national security strategies 180
3.2. Information warfare in practice 185
3.2.1. Cyber attacks against Estonia. Who is the culprit? 186

3.2.2. The Russia–Georgia conflict 194
3.2.3. Ukraine 214
3.3. Comments 220
3.3.1. Characteristics of the Russian idea of information warfare 220
3.3.2. Aggressiveness 222
3.3.3. Type of Cold War 223
3.3.4. Challenges, objectives and targets 224
3.3.5. Psychological information warfare 229
3.3.6. Players of information warfare 233
3.3.7. Hybrid warfare and information warfare 236
3.3.8. Information warfare: what is new… 240

Chapter 4. Concepts and Theories: Discussions 247

4.1. Doctrines 247
4.2. Information warfare: definitions, models 256
4.2.1. The information environment 257
4.2.2. Definitions and models for information warfare 261
4.3. Information warfare or data warfare? 281
4.3.1. Defining data 284
4.3.2. Some theories about data 289
4.3.3. Visualization 296
4.3.4. Data warfare? 306

Conclusion 325

Index 329

Introduction

The issue of information warfare was at the heart of the debate about the revolution in military matters, from the turn of the 1980s to the 1990s. It was not so much a question of doubt as to the actual relevance of the concept (the importance of information in warfare has been well known for centuries), as a redefinition of the way in which military strategy was to be viewed, in light of a radical technological and societal transformation, and how that information was now to be produced and used in these contexts.

The concept of "information warfare" appears to be used less nowadays than it once was, but it is by no means obsolete.

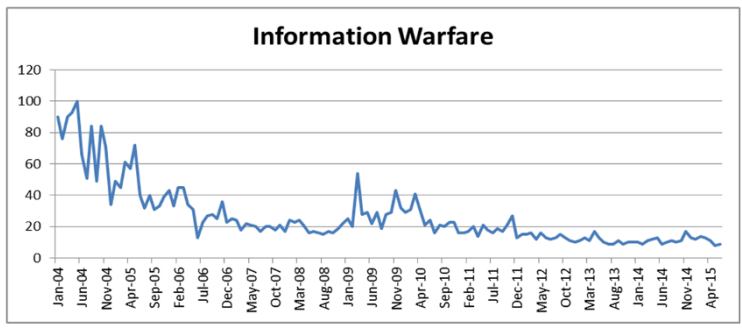


Figure I.1. *Google Trends. Evolution in number of searches for the term "Information Warfare"*[1]

1 Data harvested on 13 July 2015.

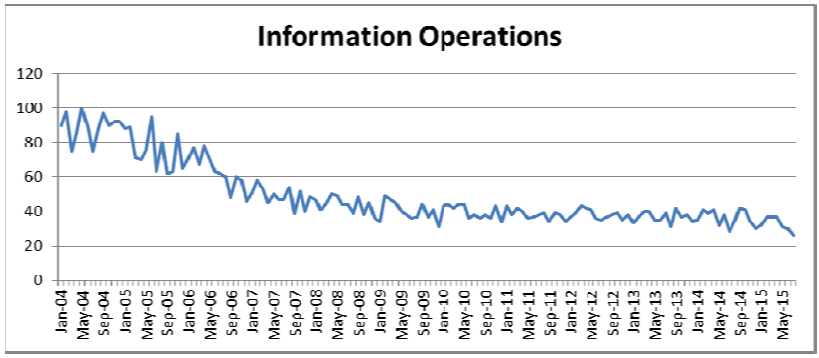


Figure I.2. *Google Trends. Evolution in number of searches for the term "Information Operations"*[2]

Certainly, the Defense Department officially removed the term from its vocabulary in 2006. However, whilst the US Army opts to use other formulations, information warfare is still the subject of theorizing, expansion, description and analysis. The concept is still used in the military world, including in the United States[3]. Numerous publications (books, reports and articles) have been devoted to information warfare in recent years, which is indicative of the interest it continues to arouse and its relevance in strategic debates (Roland Heickerö, 2010[4]; Wang Rong-Hui, Jin Li-Ya, Yuan Yi, 2010[5]; J. Martins *et al.*, 2012[6]; William Hutchinson, Matthew Warren,

2 Data harvested on 13 July 2015.

3 Isaac R. Porche III, *et al.*, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, Rand Corporation, United States, p. 178, 2013, http://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf.

4 Roland Heickerö, "Emerging cyber threats and Russian views on information warfare and information operations", *Swedish Defence Research Agency*, p. 70, March 2010, http://www.foi.se/ReportFiles/foir_2970.pdf.

5 Wang Rong-Hui, Jin Li-Ya, Yuan Yi, "Thinking about equipment support for information warfare", *Journal of Academy of Armored Force Engineering*, China, vol. 24, no. 4, pp. 20–24, August 2010.

6 J. Martins *et al.*, "Information Security Model to Military Organizations in Environment of Information warfare", *Proceedings of the 11th European Conference on Information Warfare and Security*, Laval, France, Academic Publishing International Limited, United Kingdom, pp. 186–93, 2012.

2012[7]; K. Prislan, I. Bernik, 2012[8]; Alan Chong, 2012[9]; He Su-Hong, Chen Lei, 2012[10]; Brett van Niekerk, Manoj S. Maharaj, 2011[11]; Roland Heickerö and Martin Peterson, 2012[12]; Derek S. Reveron, 2012[13]; Khurshid Khan, 2012[14]; Monika Chansoria, 2012[15]; Richard A. Poisel, 2013[16]; Daniel Gold, 2013[17]; Isaac R. Porche III *et al.*, 2013[18]; William Hagestad, 2013[19]; Alan Chong, 2013[20]; Michael

7 William Hutchinson, Matthew Warren, *Information warfare*, Routledge, May 2012, p. 224, 2012.

8 K. Prislan, I. Bernik, "From Traditional Local to Global Cyberspace – Slovenian Perspectives on Information warfare", *Proceedings of the 7th International Conference on Information warfare and Security*, Seattle, USA, Academic Publishing Limited, UK, pp. 237–44, 2012.

9 Alan Chong, "Singapore's Encounter with Information Warfare: filtering electronic globalization and military enhancements", in Daniel Ventre (ed.), *Cyber Conflict: Competing National Perspectives*, Wiley, 2012.

10 He Su-Hong, Chen Lei, "Research on complex network topology model based information warfare system", *Proceedings of the 9th International Conference on Fuzzy Systems and Knowledge Discovery*, Sichuan, China, Piscataway Publishing, pp. 2228–2231, 2012.

11 Brett van Niekerk, Manoj S. Maharaj, "The Information Warfare Life Cycle Model", *South African Journal of Information Management*, vol. 13, no. 1, pp. 97–105, March 2011.

12 Roland Heickerö and Martin Peterson, *The Dark Sides of the Internet: On Cyber Threats and Information warfare*, Peter Lang GmbH, Internationaler Verlag der Wissenschaften, p. 170, November 2012.

13 Derek S. Reveron, "Persistent enemies and cyberwar: rivalry relations in an age of information warfare", *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, pp. 139–157, Washington: Georgetown University Press, p. 19, 2012.

14 Khurshid Khan, "Understanding information warfare and its relevance to Pakistan", *Strategic Studies*, vol. 32/33, no. 4/1, pp. 138–159, Winter 2012/Spring 2013.

15 Monika Chansoria, "Defying borders in future conflict is East Asia: Chinese capabilities in the realm of information warfare and cyberspace", *The Journal of East Asian Affairs*, vol. 26, no. 1, pp. 105–127, 2012.

16 Richard A. Poisel, *Information Warfare and Electronic Warfare Systems*, Artech House Electronic Warfare Library, p. 414, 2013.

17 Daniel Gold, *Information Warfare on an Evolving Battlefield*, Montezuma Publishing, p. 122, January 2013.

18 Isaac R. Porche III, *Redefining Information Warfare Boundaries for an Army in a Wireless World*, Rand Corporation, USA, p. 176, 2013.

19 William Hagestad, *Chinese Information Warfare Doctrine Development 1994 – 2014*, Red Dragon Rising Publishing, p. 382, November 2013.

20 Alan Chong, "Information Warfare? The case for an Asian perspective on Information Operations", *Armed Forces & Society*, Singapore, 2013.

Raska, 2013[21]; Danny Bradbury, 2013[22]; Stephen Blank, 2013[23]; Tim Stevens, 2013[24]; V.I. Kuznetsov *et al.*, 2013[25]; Zhanshan Ma, 2013[26]; Andrew Jones, Gerald L. Kovacich, 2014[27]; Larry Wortzel, 2014[28]; Dean A. Nowowiejski, 2014[29]; Michael Raska, 2014[30]; Luciano Floridi and Mariarosaria Taddeo, 2014[31]; N.V. Lapotina, 2014[32]; Haroro J. Ingram, 2014[33]; Timothy Thomas, 2014[34]; Thomas S. Hyslip,

21 Michael Raska, "Information Warfare 3.0: weapons of mass effectiveness", *The Nation*, 3 July 2013, http://www.nationmultimedia.com/opinion/Information-warfare-3-0-Weapons-of-mass-effectiven-30209538.html.

22 Danny Bradbury, "Information warfare: a battle waged in public", *Computer Fraud & Security*, pp. 15–18, June 2013.

23 Stephen Blank, "Russian information warfare as domestic counterinsurgency", *American Foreign Policy Interests*, vol. 35, no. 1, pp. 31–44, Jan/Feb. 2013.

24 Tim Stevens, "Information warfare: a response to Taddeo", *Philosophy & Technology*, vol. 26, no. 2, pp. 221–225, June 2013.

25 V.I. Kuznetsov, "Electronic warfare and information warfare: how they compare", *Military Thought*, vol. 22, no. 1, pp.1–9, 2013.

26 Zhanshan Ma, "First passage time and first passage percolation models for analysing network resilience and effective strategies in strategic information warfare research: a brief survey and perspective", *International Journal of Information and Computer Security*, Inderscience Enterprises, Switzerland, vol.5, no.4, pp. 334–58, 2013.

27 Andrew Jones, Gerald L. Kovacich, *Global Information Warfare: The New Digital Battlefield*, Second Edition, Auerbach Publications, 2nd edition, p. 384, October 2015.

28 Larry Wortzel, *The Chinese People's Liberation Army and Information Warfare*, CreateSpace Independent Publishing Platform, p. 80, March 2014, http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1191.pdf.

29 Dean A. Nowowiejski, *Concepts of Information Warfare in Practice: General George S. Patton and the Third Army Information Service*, Aug.-Dec. 1944, Pickle Partners Publishing, September 2014, p. 48.

30 Michael Raska, Rethinking information and cyber warfare: global perspectives & strategic insights, Conference Report, Rajaratnam School of International Studies, Singapore, p. 30, 3 March 2014, http://www.rsis.edu.sg/wp-content/uploads/2014/11/ER140527_Rethinking_Information.pdf .

31 Luciano Floridi and Mariarosaria Taddeo, *The Ethics of Information Warfare*, Springer, p. 211, March 2014.

32 N.V. Lapotina, "The modern information culture and information warfare", *Scientific and Technical Information Processing*, vol. 14, no.3, pp. 155–158, July 2014.

33 Haroro J. Ingram, "Three traits of the Islamic State's Information Warfare", *RUSI Journal: Royal United Services Institute for Defence Studies*, vol. 159 no. 6, pp. 4–11, p. 8, Dec 2014.

34 Timothy Thomas, "Russia's information warfare strategy: can the Nation cope in future conflicts?", *Journal of Slavic Military Studies*; vol. 27, no. 1, pp. 101–130, Jan-Mar 2014.

2015[35]; M.N. Sirohi, 2015[36]; Patrick Molenda, 2015[37]; M. Jaitner, P.A. Mattsson, 2015[38]). All these publications deal with the concept in its civil and military dimensions, using approaches taken from strategic studies, political science, information sciences, computing/telecoms, and judicial, ethical and philosophical thinking. They set out to explain the profound changes that have come about in the modern field of battle, because of the evolution of the information space – its continuous and accelerated expansion over the past two decades. A number of these works are based on observations of national strategies in regard to information warfare (the conflict between North and South Korea, Russia, China, etc.).

Information warfare – though military doctrine today rather favors the concept of "information operations" – is demonstrably an essential component in modern conflicts. This is attested by recent events such as Russia's annexation of Crimea or Daesh's growing influence on the international scene, and the efforts made by certain states to counter terrorist propaganda. Both State- and non-State actors in conflicts are constantly investing in the informational sphere, placing their actions of communication, influence, propaganda, their psychological operations, at the heart of their strategies. Today, "information warfare" and "cyber" overlap. In addition, it is on this "cyber" aspect of information warfare which we focus in this book. The questions and issues are identical to those that were present in the 1990s: how best to take advantage of information and of information technologies, to gain an edge over the adversary, the enemy or the competitor. The starting point for our study in the first edition of this book (2007 in French; 2009 for the English-language equivalent) was the Gulf War (1991), reflecting how important a milestone that war was in the

35 Thomas S. Hyslip, *Bit Wars: Cyber Crime, Hacking & Information Warfare* (Volume 2), CreateSpace Independent Publishing Platform, p. 98, June 2015.
36 M.N. Sirohi, *Cyber Terrorism and Information Warfare*, Alpha Editions, p. 306, May 2015.
37 Patrick Molenda, "Silence on the Net", *U.S. Naval Institute Proceedings*, vol. 141, no. 347, pp. 34–39, May 2015.
38 M. Jaitner, P.A. Mattsson, "Russian Information Warfare of 2014", *Proceedings of the 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon)*, Tallinn, Estonia, pp. 39–52, 2015.

history of conflicts. It allowed the Americans to demonstrate astonishing might and military efficiency, and marked the beginning of a new era of conflict where information, computer systems and networks would play a major role in the organization and manifestation of that power. Numerous countries then launched a process of reflection to restructure and reorganize their forces. Although the American power could not be rivaled, it nonetheless served as a model, which at least provides the key conceptual elements. It was during the 1990s that the majority of the key concepts which are employed today in conflict strategies – and especially cyberconflict strategies – were lain down, formulated and defined: network-centric warfare (NCW), netwar, information warfare (IW), cyber warfare and big data, to cite just a few. The concept of "information warfare" has met with varying degrees of success from one State to another, and has even been officially withdrawn from the lexicon used by the US Defense Department. However, in today's world, where the strategies employed include concepts such as the influence of the media and social networks in the organization of armies and in the conducting of conflicts; where they include concepts such as psychological warfare in combination with the use of the media, propaganda, influence; where States at war or experiencing periods of revolt or insurrection impose censorship and cut off Internet access; where intelligence agencies trawl cyberspace in search of strategic information, or collect vast masses of data to be processed, analyzed, made to "talk" and support the missions of security and national defense; everyone is involved in the quest for information mastery. When these activities take place in the context of armed conflicts, between different States or within a State, we speak of information warfare.

Recent years have seen a drastic increase in armed conflicts (i.e. wars, though theoreticians, politicians or strategists often refuse to use that term), all of which have confirmed the importance of the role of information – especially information travelling through cyberspace: examples include the Russo–Georgian conflict in 2008, the Arab Spring wave of revolutions in 2010–2011, the war in Libya, in Syria, the expansion of Islamic State-controlled territory, the Russian–Ukrainian conflict, etc.

This second edition of the book focuses on three states: the USA (Chapter 1), China (Chapter 2) and Russia (Chapter 3), and offers a detailed analysis of the evolution of the theories, concepts and doctrines employed in those countries (Chapter 4). In this book, which is intended to be a modest contribution to the strategic study of modern conflict, we discuss the following questions:

– Today, do the terms "information warfare", "information operations" and "cyberoperations" all denote the same reality?

– Do states perceive and talk about the same threats today as they did 20 years ago?

– Do the actors, principles and logics of information warfare still remain the same?

1

The United States

The United States proved the undeniable power of their military with Desert Storm in 1991. Since then, their modern military and combat styles have served as examples to the rest of the world. Of course, the impressive volume of troops deployed to conquer Iraq explained, in part, their victory against an inadequate military. But what people have retained is the new face of war: information is now at the forefront and its "digital" nature clearly provides a new power to its users. Not only could the planet watch the launching of operations in real time, but optimized use of information and communication technologies to help troops, and the coordination and preparation of operations and the carrying out of attacks proved to be, if not the key to victory, at least a major player in not losing. The lessons drawn from this victory raised several questions: was this a new type of war? Should we call it "information age warfare" or "information warfare"? This first chapter is naturally dedicated to the United States, since they have been used as a reference and as an object of observation for the rest of the world. They have also put forward a series of doctrinal texts and innovative concepts in the last 25 years.

1.1. Information warfare in the 1990s

1.1.1. *Points of view from security experts*

In 1994, in his book *Information Warfare* Winn Schwartau, security expert and author of many reference publications in the field

Information Warfare, First Edition. Daniel Ventre.
© ISTE Ltd 2016. Published by ISTE Ltd and John Wiley & Sons, Inc.

of information technologies, defined three categories of information warfare:

– personal information warfare (called Class 1 information warfare), created through attacks against data involving individuals and privacy: disclosure, corruption and intercepting of personal and confidential data (medical, banking and communications data). These attacks aimed at recreating or modifying the electronic picture of an individual by illicit means, or simply by using available open-source information, can often be simply carried out through technical solutions for standard catalog or Internet sales;

– commercial information warfare (called Class 2 information warfare) occurs through industrial espionage, broadcasting false information about competitors over the Internet. The new international order is filled with tens of thousands of ex-spies looking for work where they can offer their expertise;

– global information warfare (called Class 3 information warfare) aimed at industries, political spheres of influence, global economic forces, countries, critical and sensitive national information systems. The objective is to disrupt a country by damaging systems including energy, communications and transport. It is the act of using technology against technology, of secrets and stealing secrets, turning information against its owner, of prohibiting an enemy from using its own technologies and information. It is the ultimate form of conflict in cyberspace occurring through the global network. This class of information warfare generates chaos.

According to Winn Schwartau[1], real information warfare uses information and information systems as a weapon against its targets: information and information systems. This definition eliminates kinetic weapons (for example bombs and bullets). Information warfare can attack people, organizations or countries (or spheres of influence)

1 Schwartau W., *Information Warfare – Chaos on the Electronic Superhighway,* New York, Thunder's Mouth, Press, 1994 (1st edition) and for more recent approaches SCHMIDT M.N., *Wired Warfare:Computer Network Attack and jus in bello,* RICR, vol. 84, no. 846, pp. 365–399, www.icrc.org/Web/eng/siteeng0.nsf/3e02cd6224ce0af61256, June 2002 and SCHWARTAU W., *Information Security*, Rodney Carlisle(ed.), Encyclopedia of Intelligence and Couterintelligence, 2005.

via a wide range of techniques, such as breach of confidentiality, attacks against integrity, psychological operations and misinformation.

Information warfare is therefore not limited to the military sphere: it can be carried out against civil infrastructures, constituting a new facet of war where the target can be the national economic security of an enemy. On the other hand, methods for carrying out a war are not a military monopoly. A small group of antagonists can launch an information warfare offensive remotely, while comfortably seated in front of a computer and completely anonymous. A group of hackers could choose to declare war against a country, independently from any control of State power.

For Al Campen[2], U.S. Air Force Colonel, one of the main criteria for defining information warfare is what is different from the past; this difference involves dependence on a vulnerable technology (information technology). Al Campen[3] limits the field of information warfare to information (data) in its digital form and to the software and hardware responsible for its creation, modification, storage, processing and distribution. From this point of view, psychological operations[4] consisting of scattering leaflets over populations are not information warfare operations; public broadcasting and electronic manipulation of television images, however, are part of information warfare. The physical destruction of telecommunications devices is not information warfare, but disrupting or paralyzing communication with the help of a virus is.

For James F. Dunningan[5], information warfare is attacking and defending the capability of transmitting information[6].

---

2 Thrasher R.D., *Information Warfare Delphi:Raw Results*,Naval Postgraduate School, Monterey, California, USA, June 1996, 56 pages. http://www.iwar.org.uk/iwar/resources/usnavy/delphi.pdf.

3 See Campen A.D., *The First Information War: The Story of Computers and Intelligence Systems in the Persian Gulf War*, AFCEA International Press, 1992 and Campen A.D., *Cyberwar*, Washington DC, AFCEA Press, 1996.

4 This concept is addressed in more detail later in this chapter.

5 Read DUNNINGAN J.F., *Digital Soldier: The Evolution of High-Tech Weaponry and Tomorrow's Brave New Battlefield*, St. James Press, New York, 1996, First Edition, p. 309.

For Fred Cohen, information technology security expert and inventor of the concept of the "computer virus"[7], information warfare is a conflict in which information or information technology is the weapon, target, objective or method[8].

Martin C. Libicki[9] defines information warfare as a series of activities triggered by the need to modify information flows going to the other party, while protecting our own; such activities include physical attack, radio-electronic attack, attacks on systems and sensors, cryptography, attacks against computers, and psychological operations. His definition is not limited to military information warfare. In 1995, Libicki wondered about the nature of this new concept: was it a new form of war, a new art, or the revisited version of an older form of war? A new form of conflict that would exist because of the global information infrastructure, or an old form that would find new life with the information age? Is information warfare a field by itself? In order to attempt to define the parameters of this concept, Libicki identifies seven major components:

– command and control warfare (C2);

– intelligence warfare;

– electronic warfare;

– psychological operations;

– hacker warfare (software attacks against information systems);

– economic information warfare (through the control of commercial information);

– cyber warfare (i.e. virtual battles).

Some aspects of information warfare are as old as time: attempting to strike at the head of the enemy (C2 war), carrying out all sorts of deceptions (deceiving, abusing and misleading the enemy), and

6 Thrasher R.D., 1996.
7 See http://all.net/contents/resume.html as well as http://www.iwar.org.uk/cip/resources/senate/economy/cohen~1.htm
8 Thrasher R.D., 1996.
9 http://www.rand.org/about/contacts/personal/libicki/.

psychological operations. On the other hand, hacker warfare and cyber warfare are completely new methods linked to the revolution of information and communications technologies.

For Larry Merritt[10], technical director for the Air Force Information Warfare Center (AFIWC), information warfare includes all actions undertaken to exploit or affect the capacity of an adversary to acquire a realistic image of the battlefield or to operate the command and control of his or her troops. Information warfare also includes actions undertaken for the protection of our own capabilities; electronic warfare, computer network attacks, intelligence, reconnaissance and surveillance are all defensive actions.

The concept of "information warfare" creates multiple approaches which can be very different. The reason is in the nature of the terms making up the expression: what is "warfare", what is "information"? The problem in defining the semantic parameters has led to the different points of view on information warfare.

Regardless of the approach, information warfare seems closely linked to our new social and technical structure, to the strong dependence now linking our exchanges (our social, economic, cultural and political transactions) to information technologies. Information warfare could be a type of battle for the control of the digital space involving the whole of society. Information and information systems can be used to attack and conquer the enemy. Some would prefer to call it "information age warfare" to define the capacity to control and use the information battlefield, which then becomes an additional factor in the war, in the same way that the capacity to control air and space did in conventional wars in the industrial age.

The major point that seems to define the debate on information warfare is framed by the following questions: can the war be carried out only in the world of information? Are wars, as fought by man since the beginning of time with their streams of increasingly lethal weapons and bloody battles, on the verge of disappearing? Will information technologies revolutionize societies to the point of

10 Thrasher R.D., 1996.

revolutionizing the way we fight wars, i.e. imposing our political will on others only through battles in the information sphere? Or will they only be a new complementary method? Should we call it "information warfare" or "information age warfare"?

The information space, understood as a space of violence, conflict and battle completely replacing the more traditional fields of conflicts, is one of the major ideas in the development of the "information warfare" concept: "Information technology is the most relevant basis for modern warfare. It has become conceivable to fight a war solely with information, which is expressed by the term 'information warfare' […]. Information warfare could be defined as comprising all the means of accomplishing and securing information dominance so as to support politico-military strategies by manipulating adversary information and information systems and simultaneously securing and protecting one's own information and information systems, and increasing their efficiency"[11].

1.1.1.1. *Official military documents*

It is impossible to list all the publications, reports, commentaries, analyses, opinions and notices published and expressed by experts of all fields on the subject since the beginning of the 1990s.

But in order to gain the best possible understanding of what the United States means by "information warfare", it is necessary to understand military doctrines which have endeavored to provide the definitions of key concepts, while keeping in mind the pragmatic needs of defense. The idea is not to theorize but to provide the military with guidelines and precise frameworks for their organization, strategies, operations and tactics.

The text that formally launched the concept of information warfare is a classified guideline of the Department of Defense (DOD), from 1992[12].

---

11 Elisabeth Hauschild, "Modern and information warfare: A conceptual approach", in *International Security Challenges in a Changing World* (*Studies in Contemporary History and Security Policy,* vol. 3), K.R. Spillmann & J. Krause, (eds); see: http://www.isn.ethz.ch.

12 DoD Directive TS-3600.1, December 21, 1992, "Information Warfare".

Subsequent evolutions, however, enhanced the concept before it finally found its place within the different American military doctrines.

In an instruction from January 1995[13], the Navy defined information warfare as an action taken to support the national security strategy[14] in order to reach and maintain a decisive advantage, by attacking the information infrastructure of the enemy, by using, paralyzing or influencing opposite information systems while protecting friendly information systems. For the American Navy, the term "information warfare" means that ICTs are a force multiplier authorizing more efficient operations: more efficient electronic warfare, better cryptology. The military can carry out the same operations as before but in a better way. ICTs provide improvement compared to the past. This improvement attracts more attention than the idea of radical transformation of ideologies, objectives or targets.

The Air Force document called "The Foundation of Information Warfare"[15] makes a distinction between information age warfare and information warfare: the former uses computerized weapons and the latter uses information as a weapon, an independent field.

The Army, Navy and Air Force do not share a common doctrine. This trend will be more obvious in the coming years.

1.1.2. *US Air Force Doctrine: AFDD 2-5 (1998)*

In August of 1998, the US Air Force published its doctrine on information operations (Air Force Doctrine Document – AFDD 2-5 –

13 Instruction 3430.26, Department of the Navy, Washington DC 20350-2000, OPNAVINST 3430.26, No 6, 18 January 1995.

14 The strategy consists of defining fundamental long term goals and choosing action methods and resources necessary for the achievement of these objectives. It is the part of military science involving the general behavior of the war and the defense organization of a country. It is the art of making an army evolve through operations until it is in contact with the enemy. The tactic is the application of the strategy, all the methods used to achieve a short term result. It is the art of combining all military methods to achieve goals.

15 WOOD R., The Foundation of Information Warfare, Research Report, Maxwell AFB, Air War College, 1995.

Information Operations[16]). Examining the content of this document with a comparative analysis of the official doctrine of the Joint Chiefs of Staff (JCS) (JP 3-13)[17] published the same year is interesting, as will be seen in section 1.1.3.

How is information warfare defined in this doctrine from the US Air Force? What are its components? Which concepts must be compared with the concept of information warfare?

1.1.2.1. *Superiority of information*

Superiority of information is the degree of dominance in the field of information providing friendly forces the possibility of collecting, controlling, using and defending information without actual opposition.[18]

Superiority of information, as considered by the Air Force, is a state of relative advantage, and not a capacity as presented in JP 3-13.

1.1.2.2. *Information operations*

This term groups actions taken to conquer, use, defend or attack information and information systems, including "information-in-warfare" and "information warfare" simultaneously. Information-in-warfare means conquering (acquiring) information and using it. Information warfare means attacking and defending.

1.1.2.3. *Information warfare*

Information warfare is made up of information operations carried out to defend our own information and our own information systems, or to attack and affect the information and information systems of an enemy. The definition introduces concepts that will not be found in the (JCS) approach (JP 3-13): the concept of counter-information and its two subsets of offensive counter-information and defensive

16 http://www.ttic.mil/doctrine/jel/service_pubs/afd2_5.pdf.
17 Joint Pub 3-13. Joint Doctrine for Information Operations, 9 October 1998. Joint Chiefs of Staff. p. 136,
http://www.c4i.org/jp3_13.pdf.
18 Air Force Doctrine Document 2-5, August 5, 1998, http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf.

counter-information. Counter-information establishes the desired level of control over functions of information, enabling friendly forces to operate at a given moment and place, without prohibitive interference from the adversary.

Offensive counter-information group offensive operations in information warfare, carried out to control the information environment by paralyzing, deteriorating, interrupting, destroying or attempting to deceive information and information systems include:

– psychological operations (the definition adopted is the same as the one subsequently published in the JP 3-13 document);

– electronic warfare (the definition adopted is the same as the one published in the JP 3-13 document);

– military deception;

– physical attacks (the definition adopted is the same as the one in JP 3-13);

– information attack: an action taken to manipulate or destroy enemy information systems without visibly changing the physical entity in which they reside. This means attacking the content without leaving a visible trace on the outside. The closest term is CNA (Computer Network Attacks)[19] in JP 3-13. The JP 3-13 document includes computer destruction.

Defensive counter-information group activities carried out to protect and defend friendly information and information systems include:

– information assurance;

– operations security;

– counter-intelligence;

– psychological counter-operations;

19 The abbreviation CNA will be used throughout this book.

– counter-deception;

– electronic protection.

1.1.3. *The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (1998)*

Information warfare is also defined in a publication from the JCS on October 9, 1998, called Joint Pub 3-13 "Joint Doctrine for Information Operations (IO)"[20]. The JCS text was published after the Air Force document. This detail is important because the JCS publication is intended, theoretically at least, to apply to all departments. Since the "Goldwater-Nichols Department of Defense Reorganization" Law[21] of 1986, each department must ensure the compliance of its doctrine and procedures with the common doctrine established by the JCS. Information operations doctrines, however, were developed concurrently.

The JCS publication provides the doctrinal basis for the conduct of information operations during joint operations.

1.1.3.1. *Superiority of information*

Acquiring "superiority of information" means being able to collect, process and distribute an uninterrupted flow of information, while using or blocking the possibilities of an opponent to do the same.

Document JP 3-13 defines superiority of information as absolute perfection, with the idea of "uninterrupted flow of information" for friendly forces, banning this flow to the enemy. The U.S. Air Force is not seeking such an absolute, considering instead that operations in the field of information cannot be perfect. It prefers to speak of "relative advantage": opponents will try to disrupt information operations, but Air Force superiority of information will ensure that these attempts are unsuccessful.

20 http://ics.leeds.ac.uk/papers/pmt/exhibits/469/jp3_13.pdf.
21 http://www.ndu.edu/library/goldnich/99433pt1.pdf.

The components of superiority of information are also different, and the common components are structured differently. For JP 3-13, there are three components: information systems, relevant information and information operations. The Air Force only has one component for superiority of information: information operations.

1.1.3.2. *Information operations*

Information operations are the actions taken to affect the information and information systems of the enemy, while defending our own information and information systems. There are two main sub-divisions in information operations: offensive information operations (gain) and defensive information operations (exploitation)[22]. Remember that for the Air Force, the two sub-divisions of information operations are information warfare and information-in-warfare.

For JP 3-13, the expression "offensive information operations" means actions aimed at affecting adversary decision-makers in reaching or promoting specific objectives. For the Air Force, offensive activities of information warfare are carried out to control the information environment.

The objective of offensive information operations, which can be carried out in a wide range of military operation situations, at all levels of warfare (strategic, operational and tactical) and that can have an even greater impact when carried out in times of peace or at the beginning of a conflict, is to affect enemy decision-makers or to reach specific goals. Offensive activities include, among others:

– operations security;

– military deception (deceive, trick, and set the enemy up to act against his or her own interests);

– psychological operations;

– electronic warfare;

– physical attack, destruction;

22 Page vii, JP 3-13.

– special information operations;

– computer attacks.

Defensive information operations integrate and coordinate policies, procedures, operations, resources and technologies for the defense and protection of information and information systems. They must ensure necessary protection and defense of information and information systems that joint forces depend on to carry out their operations and reach their objectives. They consist of:

– information assurance (IA);

– operations security;

– physical security;

– counter-deception;

– counter-propaganda;

– counter-intelligence;

– electronic warfare;

– special information operations.

Defensive and offensive operations are complementary and support each other. Offensive operations can support defensive operations through four processes:

– protecting the information environment;

– detecting attacks;

– restoration capabilities;

– responding to attacks.

Because of their relationship, it is important that all offensive and defensive operations components are integrated. If, theoretically, defensive and offensive are separate, in reality they must be designed and taken as inseparable.

The report also identifies “special information operations”, a category of information operations that requires detailed examination

and a process of approval because of their sensitivity, their effect or impact potential, their security needs or risks to the national security of the United States.

1.1.3.3. *Information warfare*

The superiority of information diagram, according to JP 3-13, does not include information warfare, which is only defined as the series of operations carried out during a crisis or conflict to reach or promote specific objectives over one or more specific adversaries[23]. Information warfare therefore is a subset of information operations: simply operations conducted in times of crisis or conflict. In times of peace, we could not speak of information warfare. But the doctrine does not define the notions of "crisis" and "conflict" either.

This definition is quite different from the Air Force's definition.

In both approaches, information warfare is an information operation. But even though JP 3-13 separates information warfare and information operations according to the time space in which they occur, the Air Force considers that we are constantly in a state of information warfare because the defensive side is always engaged. This approach (from the US Air Force) may seem more relevant considering the situation after over ten years. The United States (and many other nations) are the subject of permanent attacks launched against their information space (targeting the Pentagon and sensitive infrastructures of the country through massive and coordinated distributed denial of service (DDoS) attacks in increasing intensity since 2005), imposing a state of permanent defense, a cyber security and cyberdefense strategy applied to all levels of the grid, i.e. to civilian and military information infrastructures. This defense must be engaged despite the absence of specificly known enemies, in a period where peace, crisis and conflict are mixed without clear temporal boundaries.

Information operations cover peace and returning to peaceful periods because of their presumed deterrant character, which should

23 Page 23 in the document.

also apply to adversaries in times of crisis, making them hesitate in initiating actions. The ultimate objective of information operations remains to affect enemies or potential enemies, so that they put a stop to actions threatening the American national security interests. The 1998 text obviously did not take into account the terrorist threat. The question still remains today: can information operations be efficient enough to dissuade or intimidate any type of adversary? The dissuasive character seems implausible. The main quality of the information space is to provide any type of attacker with the ways to bypass security and defense methods. No nation, military or police force has been able to implement totally dissuasive measures against determined players. The main reason resides in the operation of networks ensuring invisibility and thus impunity to all who want to become attackers. In 2009, it seems that the computer weapon as bypass weapon, and certainly not as a weapon of dissuasion, was an accepted fact.

1.1.4. *Components of information warfare*

It is necessary at this point to explain in more detail the fundamental concepts discussed previously, particularly those called components of information warfare that we invariably find in the different doctrines which are formulated in the United States, but also all over the world. They are psychological operations (PSYOPS), electronic warfare, military deception, operations security (OPSEC), information assurance (IA) and computer network attacks (CNA).

1.1.4.1. *Psychological operations*

The sub-title of this section could be “The importance of psychology in battles between individuals or groups of individuals”. PSYOPS emerged way before the digital age and will probably outlive it. They can be summarized as the use of communication to influence behavior.

Communication is the process by which an individual influences another person, involving the spectrum of human actions (speaking, writing, etc.). Theories of communication (particularly those of

Melvin L. Defleur for whom communication is the group of methods making it possible to exert social control, allocate roles and coordinate efforts) provide more detail. Communication is a tool for relations, not only between individuals, but also for individuals with their historical perspectives. Communication consists of:

– controlling the media to control received and broadcast information; filtering real information, real but partially presented information (scaling of facts), creating and broadcasting false information. The presence of the media in the field during conflicts, or close to a conflict, makes it possible for PSYOPS to take action contributing to the success of military operations, as long as the media can be controlled;

– manipulating minds through information;

– using the emotional impact of words, images, speeches or sounds;

– launching "positive propaganda" operations intended for our own camp, and "intoxication" operations aimed at the enemy.

PSYOPS by misinformation, intoxication, deception, banning and propaganda[24] are incredibly important in a period of conflict because they contribute to the success of military operations, help in dominating the opponent, are used to attempt to dissuade the enemy from pursuing the fight, get him to surrender weapons and to surrender himself, help in preserving the morale of our own troops, and also help in getting and maintaining support from the population and national and international public opinion.

PSYOPS also attempt to reach thoughts, opinions, beliefs and emotions in order to influence behaviors, attitudes and affect national interests.

PSYOPS operation applications have led to the idea of the "noosphere", a field in which dominance of ideas, instead of dominance over land or populations, would be predominant.

---

24 For more information on the term "propaganda", refer to Chomsky N., *Propaganda*, Du Félin Editions, 2002.

The implementation of PSYOPS presumes a deep knowledge of theories of communication and information, psychology of individuals, their behaviors and cultures. Nobody can pretend to really understand the direct or indirect impacts of these operations today.

1.1.4.2. *Electronic warfare*

Electronic warfare priorities are denial of service (jamming, mimicry, physical attack), deception (that can be directed at automated systems or people) and exploitation (intercepting/listening, obtaining any information with operational value from the enemy's use of his or her electronic systems).

The goal of electronic warfare is to control the electromagnetic spectrum.

The American doctrine[25] defines electronic warfare as any military action using directed electromagnetic energy to control the electromagnetic spectrum or to attack the enemy. The three main sub-divisions of electronic warfare are:

– electronic attack aimed at attacking people, equipment and installations with the purpose of eroding, neutralizing and destroying enemy combat capabilities by jamming, electromagnetic deception, the use of lasers and particle beam weapons. Attacking communications can reach different objectives: access contents, detect and destroy system nodes, jam communications to disrupt the adversary, destroy the opponent's equipment with the help of high power microwaves and send instructions instead of enemy commands (deception). Deception is one of the major tools of electronic attacks. Deceiving the enemy by manipulating his or her perception in such a way that the relevance of his or her judgment and capability of acquiring targets is reduced. Physical destruction is another important facet of electronic attack. Destruction or neutralization by jamming sensors and opposite communications is called soft kill; physical destruction is a hard kill;

25 Joint Pub 1-02 document.

– electronic protection includes systems designed to be resistant to jamming by any kind of attack. Cryptography (also called Comsec – Communications Security) is an element of electronic warfare;

– the objective of electronic warfare support is to search, intercept, identify and locate sources of electromagnetic energy in order to recognize immediate threats. Electronic support provides necessary intelligence and the identification of threats for efficient attack and protection. Electronic support includes SIGINT (signals intelligence) which is made up of Comint (communications intelligence, a collection of enemy communications such as the contents of messages and traffic data) and ELINT (electronic intelligence, which captures enemy radar signals and other non-communicating electromagnetic energy sources). Before attacking the communications of an enemy, their network of communications must be mapped out; this is the role of SIGINT that will consist of extracting information from signal masses and from network traffic. Reception equipment today is able to pick up almost all signals transmitted, locate transmitters with precision and feed databases with the signals collected. Data collected must be analyzed. We must especially be able to select the traffic because trying to collect, process and analyze everything is not practical.

Electronic weapon systems are made up of sensors (radars, infrared, and sonars), communication lines (transporting data from sensors to command and control (C2) centers) and output devices (lasers, jammers, EMP).

These systems are part of the composition of C2 networks which transmit and receive data, voice and images. Communications must be secure between army commanders and political leaders, for example, so that messages and orders are not corrupted, intercepted or blocked. There are many methods threatening this security: cryptanalysis, sabotage, subversion of personnel, robbery of material, deception, jamming (such as jamming signals transmitted from a plane to the missile it just launched), physical destruction of networks and communication equipment, interception of unsecured communications (particularly if the communication uses methods such as public or radio telecommunication networks which can be the subject of

interception), intercepting orders and replacing them with others, or using voice morphing techniques to substitute commands.

With the help of this series of methods, the military develops attack and defense strategies, which are generally a mix of possibilities.

1.1.4.3. *Military deception*

"Deception" is a series of measures designed to "deceive the enemy by manipulating, deteriorating or falsifying evidence to trigger a reaction that is detrimental to his interests"[26].

For the American military, deception is aimed at enemy decision-makers, by affecting their information collection and analysis process and with dissemination systems. This deception requires an in-depth knowledge of the enemy and his or her decision-making processes. Anticipation is one of the keys. Command must imagine the way in which they think the enemy would act at critical times in the battle. These desired actions become the objective of deception operations. Military deception focuses on the desired behavior, and not only on deceiving the mind. Camp B must get Camp A command to form an inappropriate opinion of the capabilities and intentions of the troops in Camp B, so that they make decisions contrary to their interests. Military deception operations depend on intelligence operations to identify the correct targets of the deception. We must be able to create a credible story and evaluate the efficiency of the deception plan and, to have the best chance of success for such an operation, a very small number of people may need to be kept informed, to reduce the risk of an information leak. But this type of operation may also have a disruptive effect among our own camp[27].

1.1.4.4. *Operations security*

Operations security (OPSEC) is a methodology intended to keep an adversary from accessing "critical" information involving his or her

26 Joint Publication 1-02 document.
27 For more information on the American approach, please refer to JP 3-58, *Joint Doctrine for Military Deception*. Joint Chiefs of Staff. 31 May 1996. 61 pages. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_58.pdf.

camp and allies, i.e. information necessary to correctly evaluate the capabilities and intentions of the target.

The concept of OPSEC can be analyzed in the light of the doctrine in the official document titled "Operations Security – Joint Publication 3-13.3", from 29 June 2006, which modifies the previous text from 24 January 1997, referenced 3-54[28].

This new doctrinal text establishes the rules that the American military must follow in their activities and operations. It is divided into three major chapters discussing general aspects (definitions, context), OPSEC processes and OPSEC planning, consecutively. Appendices help in the practical understanding of the illustrated concepts.

The proposed definition highlights the main characteristic of OPSECs being one of the information operations. It is a process that:

– identifies critical information in order to determine whether allied actions can be observed by enemy intelligence systems;

– determines if the information obtained by adversaries could be interpreted in such a way that would be useful to them;

– executes selected measures eliminating or reducing the possibility for the enemy to use critical allied information[29].

Security programs protect classified information. OPSEC identifies, controls and protects generally non-classified information that is associated with, or can be linked to, sensitive operations or activities.

On our side, we have:

– classified information, protected by security programs;

28 Joint-Pub 3-54, *Joint Doctrine for Operations Security*, Joint Chiefs of Staff, USA, p.79 pages, 24 January 1997. http://www.iwar.org.uk/rma/resources/opsec/JP3_54.pdf.
29 JP 3-13.3 document, page vii.

– non-classified information but which can be linked to sensitive activities or operations, then qualified as “critical” and thus must be identified and protected by OPSEC;

– “indicators”, which are a class of information associated with an activity in a significant way;

– a military that is visible to the public and enemy intelligence, in times of peace, training, drills or operations. Non-classified information, when correlated with other non-classified information, can become classified or reveal a sensitive operation.

And in the enemy camp, we find information intelligence, acquisition and exploitation systems that we have to protect against.

The OPSEC process consists of five distinct actions:

– the identification of critical information, i.e. information that is crucial to the enemy, making it possible to categorize information to only protect what is qualified as “vital”;

– the analysis of threats via intelligence, counter-intelligence and open information research and analysis to identify probable enemies. We must find the answer to the following questions: who is the enemy? What goals does the enemy have? What actions could the enemy take? What information does the enemy already have? What intelligence capabilities does the enemy have?

– the analysis of vulnerabilities via the investigation of each aspect of a planned operation to identify OPSEC indicators that could reveal critical information. The objective of OPSEC is to reduce the vulnerability of American or coalition forces with regard to the exploitation of critical information by the enemy. OPSEC applies to all military activities during operations. The following questions must be answered: which indicators of critical information that are unknown by the enemy will be created by allied activities? Which indicators can the enemy collect? Which indicators will the enemy be able to use against allied forces?

– the evaluation of risk by the analysis of vulnerabilities identified in the previous phase, and identification of possible OPSEC measures for each vulnerability. Possible measures include secrecy,

concealment, camouflage, deception, intentional diversion in relation to habits, and direct strikes against enemy intelligence systems. Technical measures (see Appendix C) consist of not giving operations information in unsecure email messages, preparing for CNAs, placing vital operational information on disk, using cryptography to protect someone's voice, data and video communications, controlling radio communication transmissions, using systems with low probability of interception and secure phone lines. Finally, we need to monitor the possible interaction of OPSEC measures; measuring OPSEC may create an indicator (concealing equipment that was not protected before may reveal the preparation of military action);

– the application of appropriate OPSEC measures by command, who must determine if the gain in security exceeds cost in resources. Then, during their execution, the enemy's reaction must be observed to determine its efficiency.

The range of the spectrum involved by OPSEC implies a large number of players: army commands, Defense Intelligence Agency (DIA), National Security Agency (NSA), the OPSEC interagency and different DoD agencies.

The major problem lies in how to delimit the moving perimeter of "critical information". Information will become "critical" according to context; one piece of information that is ordinary today can become critical because of the emergence of new events. Yesterday's ally can become today's enemy, for example. Information can be critical according to the context in which it is used, whether for counter-terrorism, hostilities, military intervention or diplomatic negotiations. Anything that is the product of the armed forces could be perceived as potentially critical. This is revealed by the bans or restrictions on military personnel being able to freely express themselves through newsgroups, chatrooms or other discussion tools and information sharing.

Annex A from JP 3-13 draws the limits of this perimeter by listing examples of "critical" information; information involving military capacities, target selection, logistic capacities, intentions, active forces and reserves, and timing of operations.

1.1.4.5. *Information assurance (IA)*

This concept groups the measures that protect and defend information and information systems by ensuring their availability, their integrity, their capacity to be authenticated, their confidentiality and their non repudiation. These measures include the restoration of information systems by incorporating protection, detection and methods of reaction[30].

For the military[31], "IA" is an information operation that protects and defends information systems by ensuring their availability, integrity, authentication, confidentiality and non repudiation. This security presumes the restoration of information systems with the incorporation of methods of protection, detection and reaction.

IA consists of the protection and defense of information and information systems against unauthorized access and modification of stored, processed and transmitted information, and against denial of service for authorized users. IA also includes the measures necessary to detect, describe and counter such threats. IA is made up of computer security and communications security, also called INFOSEC[32].

"Communication security" (COMSEC) is protection resulting from all measures taken to ban access to valuable information for unauthorized people or mislead unauthorized people in their interpretation resulting from the possession and study of information[33]. Communication security includes security by cryptography, security of transmissions and physical security of communication and information methods.

30 *National Information Assurance (IA) Glossary*. Instruction No. 4009, revised version. June 2006. 86 pages. Committee on National Security Systems (CNSS), USA. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.
31 JP 3-13 from 1998.
32 JP 3-13 from 1998.
33 JP 3-13 from 1998.

1.1.4.6. *Computer network attacks*

Definitions are provided in the doctrinal text JP 3-13, pages I-9 to I-11, GL-4 to GL-10.

Document JP 3-13 from 1998 defines computer network attacks (CNAs) as operations intended to disrupt, prohibit access to, deteriorate, destroy and steal information contained in computers, carried by computer networks, or targeting computers and networks. CNAs include all forms of attacks carried out against or by computers and computer networks.

The method of attack characterizing CNAs is data flow. An electronic attack such as the use of electromagnetic forces does not fall under the CNA category but is part of electronic attacks. For example, jamming a radar is an electronic attack, not a CNA. Propagating a computer virus is a CNA, not an electronic attack. There are many ways to develop such a computer attack: access to systems, controlling systems, destruction and distortion of data (through viruses, worms and Trojan horses), and data interception.

We also speak of cyberwar to describe these forms of aggression.

1.2. Information warfare in the 2000s

1.2.1. *Dictionary of the Department of Defense*

The dictionary of the US DoD of 2001[34] uses the definition adopted by the 1998 JP 3-13 for information warfare: a methodology of information operations.

Information operations are the actions that can be taken to distort the information and information systems of the enemy, while protecting our own information and information systems. Information operations are implemented in times of peace, crisis or

34 Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*, p. 782, 12 April 2001. The document as amended at 17 March 2009 is available at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

conflict. Those implemented only in times of crisis or conflict constitute information warfare.

On the 22 March 2007 version of the dictionary[35] the expression "information warfare" practically disappeared. We find it only in the list of abbreviations and acronyms, such as AFIWC (Air Force Information Warfare Center), FIWC (Fleet Information Warfare Center), IW-D (Defensive Information Warfare), IWSC (Information Warfare Support Center), LIWA (Land Information Warfare Activity), NIWA (Naval Information Warfare Activity) and TWI (Office for Information Warfare Support – DIA/Defense Intelligence Agency).

1.2.2. *US Air Force: AFDD 2-5 (2005) and AFPD 10-7 (2006)*

On 11 January 2005, document AFDD 2-5 "Information Operations" was published[36]. There again, as in 1998, the Air Force document was published before the document from the JCS.

The first major point to note on reading this document is that the expression "information warfare" is no longer used. Only the concept of information operations is still present, and the idea of their implementation at any time: peace, war or when returning to peace. Is the distinction between time of peace/war no longer relevant?

The acquisition and maintenance of "superiority of information" are critical tasks for commands and vital elements for kinetic and non-kinetic effect-based operations. Superiority of information is the degree of dominance in the field of information providing allied forces with the possibility of collecting, controlling, using and defending information without efficient opposition.

Information operations, carried out by the military in times of peace, war and returning to peace, are now:

– influencing operations to amplify the effects of traditional military operations, as well as for influencing in a way other than

35 Joint Publication 1-02 from 12 April 2001, revised 22 March 2007.
36 http://www.iwar.org.uk/iwar/resources/usaf/afdd2-5-2005.pdf.

by just using force. The goal is to affect the perceptions and behaviors of leaders, groups and whole populations. These operations are PSYOPS, military deceptions (MILDEC), OPSEC, counter-intelligence measures (i.e. protecting against espionage, sabotage and assassinations), counter-propaganda operations and public affairs operations;

– electronic warfare operations: attacking, defending, supporting. This is the planning, use and evaluation of military methods to obtain desired effects through the electromagnetic spectrum, to support operational objectives;

– network warfare operations: attack (NetA), defend (NetD) and support (NS). This is the planning, use and evaluation of military methods to obtain desired effects through interconnected analog and digital networks in the battle space. These operations group the series of actions previously called CNA. It is a war carried out through networks: destroying, disrupting and usurping information and information systems, and protecting against these attacks).

Information operations are the integrated use of these three capabilities, in collaboration with "integrated control enablers" (ICEs), to influence, disrupt, corrupt and usurp the human and automated decision process of the enemy while protecting our own.

The doctrine no longer speaks of "information-in-warfare" but of "integrated control enablers" (ICEs). These ICEs are not information operations but group methods of acquisition and exploitation; information operations only group defense and attack methods. ICEs must provide all available information.

ICEs include intelligence, surveillance, reconnaissance (ISR) systems, network operations (NetOps – grouping systems, network management and information security), predictive battlespace awareness, and precision navigation.

Even though we no longer speak of information-in-warfare, the characteristics of war in the information age are described, as more emphasis is now placed on influencing political and military

leaders, as well as populations, to solve conflicts. Information technologies have increased the methods of directly influencing populations and their leaders. ICTs have distributed the process of collection, storage, dissemination and processing of information. The US Air Force must use this technology as a powerful lever to acquire superiority of information and to be able to operate the cycle of decision (observe, orient, decide and act, or OODA loop) quicker than the opponent. This is what is called "decision superiority": being able to observe, orient, decide and act more quickly and efficiently than the enemy.

The AFPD 10-7 (Air Force Policy Directive) document of 6 September 2006 called "Information Operations"[37] proposes a conversion chart of terminologies used by the US Air Force and JCS in the 2006 doctrines, revealing compatibility of terms used in both approaches.

ICE	IO
Acquisition and exploitation	Defend and attack

Table 1.1. *Distinction between integrated control enablers (ICE) and information operations (IO)*

1.2.3. *The doctrine of the Joint Chiefs of Staff committee: JP 3-13 (2006)*

On 13 February 2006, JCS published the new version of the doctrinal document JP 3-13 called "Information Operations"[38].

The text eliminates the expression "information warfare" from its vocabulary. It also abandons the expressions "offensive information operations" and "defensive information operations".

The five fundamental operations of information operations are: 1) PSYOPS; 2) military deception; 3) OPSEC; 4) electronic warfare; and 5) computer network operations (including the now traditional

37 http://www.fas.org/irp/doddir/usaf/afpd10-7.pdf.
38 http://www.ttic.mil/doctrine/jel/service_pubs/afd2_5.pdf.

attack, exploitation and defense operations: computer network exploitation (CNE) and computer network defense (CND), CNA. Computer network attacks consist of paralyzing, interrupting, delaying and destroying information and/or information systems. Exploitation consists of the collection, monitoring and falsification of information. Defensive operations consist of protecting, detecting, restoring and responding.

To support these five basic methods, intelligence actions collect, analyze and provide information on the environment as well as on physical attacks, information assurance, counter-intelligence and physical security.

In the doctrine, the international dimension of operations is now taking a more significant place. Through lessons and experience learned in the past by the American military, the doctrine introduces terms such as “tribe”, “family”, “culture”, “religion” and “alliances”, absent from the 1998 version. Psychological, cultural and cognitive dimensions now occupy a central place.

Also of interest in this document is the representation of the information environment proposed by the military. Three different aspects, or dimensions, constitute the space in which the military must evolve and information operations must be carried out: a physical dimension, made up of command and control systems, infrastructures, networks and computers; an information dimension, where information is collected, processed, stored, broadcast, displayed and protected (the space of information content and flow); finally, a cognitive dimension which includes the thoughts of decision-makers and target audience: it is the space of perception, visualization, decision and thinking, and it is this dimension where battles and campaigns can be won or lost. Factors influencing the cognitive dimension are emotions, state of mind, experience, spatial awareness, public opinion, perceptions, media and rumors.

Annex B of JP 3-13 is extremely interesting because it proposes a table identifying the possible conflicts between the different actions of information operations. An attack by computer networks could be in conflict with a PSYOP if that attack prohibited the enemy from

receiving the message addressed to him or her in the context of a PYSOP. Or a CNA type attack could be in conflict with a military deception operation when, by absence of coordination between the two, the result would be attacking the wrong target. Or when, by absence of coordination, a physical attack and a software attack are launched at the same time toward the same target. This would be wasting time and ammunition.

1.3. Information warfare in the 2010s

The overview given below discusses the various doctrinal evolutions on the part of the US Army, in connection with information operations, and their proximity with cyberoperations. We focus on a number of important concepts, such as "information environment", "joint information environment" and "collaborative information environment". Our aim, in this chapter, is to illustrate the links woven between the various notions deriving from information and "cyber". The relevant documents are presented in chronological order:

– JP 1-04, Legal Support to Military Operations, 17 August 2011[39]

This publication contains the concept of a "CIE – collaborative information environment". The document introduces the idea of a CIE, but the concept is not defined in the report. It arises only rarely in American military doctrine. It does reappear in a call for tender issued by the US Air Force in 2012 (Global adaptive planning collaborative information environment – GAP CIE – sustainment and enhancement)[40].

The *information environment* is said to be cyber-centered when it is described and constructed as an environment of interconnected

39 p. 79, http://www.dtic.mil/doctrine/new_pubs/jp1_04.pdf.

40 Solicitation Number: FA8707-12-R-0014, Department of the Air Force, https://www.fbo.gov/?s=opportunity&mode=form&id=b0ab0adc7702fb06d4d0da187834712e&tab=core&_cview=1. The contract was awarded to Northrop Grumman, in 2014, for $98m (http://defensesystems.com/Articles/2014/06/02/Air-Force-Northrop-Joint-Operations-Planning-tool.aspx). The GAP CIE is a planning system, for command and strategy.

computers and systems. The concept of a "joint information environment" (JIE) expresses this convergence toward the world of cyber[41].

The idea of an information environment is connected directly to that of combat: "All the elements you have read about so far contribute to a broad, complex battle space known as the information environment, which we will now examine more closely"[42]. The document from which this quote is drawn never makes mention of cyberspace. The concept of the information environment is defined more specifically in JP 3-13.

JP 1-04 gives a lengthy description of what an information environment is:

> "The information environment is where humans and automated systems observe, orient, decide and act upon information, and is therefore the principal environment of decision making. ● Resources include the materials and systems employed to collect, analyze, apply or disseminate information. The information environment is basically made up of three interrelated dimensions: physical, informational and cognitive. Let's take a look at each one. The physical dimension is composed of the command and control systems and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, sea and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside. This includes the means of transmission, infrastructure, technologies, groups and populations. Comparatively, the elements of this dimension are the

41 http://fcw.com/articles/2012/09/13/joint-information-environment-in-combat-iphone-5.aspx.

42 Department of Defense, Public Affairs Qualification Course DoD Principles of Information and Information Environment, p. 10, https://dinfos.blackboard.com/bbcswebdav/library/Library%20Content/Public%20Affairs%20-%20PALD/DOD%20Principles%20of%20Information%20and%20Information%20Environment.pdf.

> easiest to measure, and consequently, combat power has traditionally been measured primarily in this dimension. The *informational dimension* is where information is collected, processed, stored, disseminated, displayed and protected. It is the dimension where the command and control of modern military forces is communicated and where commander's intent is conveyed. It consists of the content and flow of information. Consequently, it is the informational dimension that must be protected. The *cognitive dimension* encompasses the mind of the decision maker and the target audience. This is the dimension in which people think, perceive, visualize and decide. It is the most important of the three dimensions. This dimension is also affected by a commander's orders and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information and rumors influence this dimension."

Whilst the descriptive formulations of each of the three dimensions may differ marginally from those found in JP 3-13, the essential point remains – particularly the consensus about the overall three-level architecture. However, this approach is set apart because of how it links the information environment to the OODA loop.

– AFDD 1, Air Force Basic Doctrine, Organization, and Command[43]. 14 October 2011

The expression "information warfare" does not appear in the document. It is a question of the "information environment", in which cyberspace constitutes one domain.

Whilst cyberspace is defined in this document (reminiscent of the definition given by JP 1-02), the information environment is not.

---

43 http://www.globalsecurity.org/military/library/policy/usaf/afdd/1/afdd1-2011.pdf.

Meanwhile, a definition is given for the concept of information operations: "This mission is the integrated employment of the capabilities of influence operations, electronic warfare operations, and network warfare operations, in concert with specified integrated control enablers, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting one's own"[44].

The document devotes more space to the discussion of "cyber" than to that of information *per se*:

– AFDD 2-0, Global Intelligence, Surveillance, and Reconnaissance Operations, 6 January 2012[45]

Whilst AFDD 1 discusses the trio of air, space and cyberspace, AFDD 2-0, for its part, refers to the set of air, space, cyberspace and information operations[46]:

– Joint Information Environment White Paper, 22 January 2013[47]

This document, published by the JCS, hinges on the concept of the JIE, which is of crucial importance in the way in which the forces prepare to confront security concerns. The essential principle is the deployment of global integrated operations and the enabling of the defense forces to deal with the uncertainty, complexity and rapid change[48]. The concept of the JIE refers to an intended radical evolution in the approach to and handling of challenges – particularly those pertaining to the information environment.

One of the evolutions which seem most central pertains to the transition from a network-centric approach to a data-centric one. This evolution, which accords a major role to data (big data, cloud computing, etc.), is a profound change of paradigm. We shall discuss this approach in detail in Chapter 4 of this book. The construction of a JIE requires other evolutions to take place: improving the mastery of

44 Page 50.
45 http://www.globalsecurity.org/military/library/policy/usaf/afdd/2-0/afdd2-0.pdf.
46 Page 19.
47 http://www.jcs.mil/Portals/36/Documents/Publications/environmentalwhitepaper.pdf.
48 Page 3.

cyber by using real-time data, adapting the security and resilience of the information environment. The JIE is based on a network of data centers, a global identity-management system, the provision of services, storage systems, dissemination systems and data-access systems. The (utopian) project aims to reinforce the protection of integrity of information, by preventing unauthorized access. However, as it is impossible even to aspire to perfection – much less achieve it – in this field, great care must be exercised, and the project already prescribes the use of procedures to deal with attacks on the data. The weaknesses that need to be dealt with by these new cyberspace-based approach (vulnerabilities) are lack of interoperability, the rapid rate of technological change and the concomitant costs[49].

The information environment referred to in the JIE is essentially centered in cyberspace. Hence, it is a question of the importance of information technology and the shortcomings of cyberspace, and the data which need to be distributed, shared and rendered secure are digital data.

– JP 3-12 Cyberspace Operations, 5 February 2013[50]

The information environment is again that in which cyberspace exists.

The document adds to the definition of *cyberspace*, in comparison to that given by other sources, specifying that it is one of the five interdependent domains (alongside the air, land, maritime and space domains)[51]. Thus, here, there are at least two unique points to be highlighted: firstly that cyberspace is not alone, and secondly that it is interdependent with the other domains. Thus, there may potentially be similarities or differences to be found in relation to the other four domains, and conclusions can be drawn from that interdependent nature, which it shares with the other domains.

Unlike with other approaches in doctrinal documents, which do not linger over the definition of cyberspace, JP 3-12 reintroduces the idea

49 Page 4.
50 http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
51 Page I-2.

of the architecture of that space, and constructs it in accordance with that of the information environment, which is structured around three levels ("layers" rather than "dimensions"): "Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona"[52]. Each layer is then divided into various sub-elements:

– Physical network layer:

- geographic component,

- physical network components;

– Logical network layer:

- "elements of the network that are related to one another in a way that is abstracted from the physical network";

– cyber-persona layer:

- "the people actually on the network".

– JP1, Doctrine of the Armed Forces of the United States, 25 March 2013[53].

This document does not give a definition for information operations, or even for information itself. It does specify, however, that cyberspace is part of the information environment.[54]

– JP 3-27, Homeland Defense, 29 July 2013[55]

This document recaps that the information environment is an operational environment (in the military sense of the term). This environment includes cyberspace. However, with that said, the illustrative Figure I-3 on page I-11, which shows the operational framework of defense of territory, indicates the two objects separately.

– JP 2-0, Joint Intelligence. 22 October 2013[56]

52 Page I-2.
53 http://www.dtic.mil/doctrine/new_pubs/jp1.pdf, 172 pages.
54 Page x.
55 http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf.

The role of the intelligence services is to provide the command centers with information pertaining to each of the three dimensions of the information environment (physical, informational and cognitive) and their impact on military operations[57]. The document mentions the concept of the information environment, but overlooks that of cyberspace (only using this term once)[58].

– JP 3-24, Counterinsurgency, 22 November 2013[59]

The information environment is described using concrete examples: "relevant aspects of the information environment may include media outlets such as radio and television; Internet communications such as e-mail and social networking sites; cellular telephone and radio communication; and channels of information flow via word of mouth. The information environment also includes the infrastructure and technology that supports the various types of communication"[60]. "It is the medium through which decision making is made and disseminated"[61].

This document touches on an essential characteristic of the information environment, which other approaches tend to overlook: it is the space in which narrations and influence take place. "The most important attribute of the information environment is that it is where the actions and the messaging of all actors combine to form the narratives that impact the mental disposition of relevant actors"[62].

– JP 3-26, Couterterrorism, 24 October 2014[63]

Cyberoperations are one of the modes of information operations[64]. In this document, the information environment is mentioned only once, in the context of the definition of cyberspace. Not even once is the concept of information warfare mentioned. This document focuses

56 p. 144, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.
57 Page I-27.
58 Page IV-17, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.
59 http://www.dtic.mil/doctrine/new_pubs/jp3_24.pdf.
60 Page IV-3.
61 Page IV-13.
62 Page IV-13.
63 http://www.dtic.mil/doctrine/new_pubs/jp3_26.pdf.
64 Page x.

on the following: information operations, information sharing, information technologies, information capability and critical information requirements. Cyber is only touched upon in the context of cyberspace operations: cyberspace technology.

– JP 3-52 Joint Airspace Control, 13 November 2014[65]

This doctrine does not introduce the notions of information operations or information environment. The link which is established between cyber and information lies in the observation that defensive cyberoperations are (amongst others) methods for protecting information[66].

– JP 3-13, Information Operations. 27 November 2012, incorporating Change 1, 20 November 2014[67]

In JP 3-13 from 1998, "Information warfare (IW) is IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries" (page I-1)[68]. This approach strictly limits information warfare to times of crisis or conflict. In peace time, we can no longer speak of information warfare. Yet information operations, of which information warfare is merely a subset, are carried out in all climates (peace time, crisis, conflict and renewed peace), much like *information assurance*, *special information operations* and *intelligence* (see the graph on page I-4). This document, from 1998, does not yet include the term cyberspace. "'Information' is defined as facts, data, or instructions in any medium or form. It is the meaning that a human assigns to data by means of the known conventions used in their representation. The same information may convey different messages to different recipients and thereby provide 'mixed signals' to information gatherers and users, to include the intelligence community" (page I-9). "The 'information environment' is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself" (page I–9).

65 http://www.dtic.mil/doctrine/new_pubs/jp3_52.pdf.
66 Page II-7.
67 89 pages, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
68 http://www.c4i.org/jp3_13.pdf.

In the 2006 version of JP 3-13[69], the expression "information warfare" is officially withdrawn from the doctrine of American information operations (see page iii). Thus, it disappears from JP 1-02. Only the US Air Force has kept the expression in its AFDD 2-5: "The theory of warfare in the information environment that guides the application of information operations to produce specific battlespace effect in support of commander's objectives". This abandonment of the concept followed the discussions over the previous years about its relevance – particularly in view of the evolution of the technologies and the military armament, which facilitate far more than merely flummoxing enemy C2 systems by deception or psychological operations[70].

In the 2014 version of this document, the definition of the information environment is rendered more precise in relation to its initial formulations: "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information" (page ix). Alternatively, consider page I-1, where the information environment is analyzed as a 3-dimensional environment, comprising the physical, informational and cognitive dimensions.

---

69 JP 3-13, Information Operations. 13 February 2006: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13(06).pdf.

70 Timothy L. Thomas, "Is The IW Paradigm Outdated? A Discussion of U.S. IW Theory", *Journal of Information Warfare 2*, 3: pp. 109–116, 24 January 1997, http://fmso.leavenworth.army.mil/documents/InfoWar.pdf.

"The *information environment* is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These dimensions are the physical, informational, and cognitive (see Figure I-1). *The JFC's operational environment* is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander (encompassing physical areas and factors of the air, land, maritime, and space domains) as well as the information environment (which includes cyberspace) […] *The physical dimension* is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries […] *The informational dimension* encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information […] *The cognitive dimension* encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Defining these influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects. As such,

this dimension constitutes the most important component of the information environment."

Each dimension is centered on a particular object:

– the physical dimension is that of the "Tangible. Real world" (see diagram on page I-4);

– the informational dimension is said to be "data-centric";

– the cognitive dimension is "human-centric".

Although the informational dimension is data-centric, the doctrine draws a clear distinction between "data" and "information" (page I-3):

– "Information. Data in context to inform or provide meaning for action.

– Data. Interpreted signals that can reduce uncertainty or equivocality."

The logic of the model, then, is simple: an *environment* is made up of several *dimensions*, which are centered on a particular *object*.

Information operations are also reformulated:

> "The Secretary of Defense now characterizes IO as the integrated employment, during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" (page ix).

– JP 6-0, Joint Communications Systems, 10 June 2015[71]

An entire chapter is given over to the information environment (Chapter II).

71 http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

Cyberspace, once again, is presented as a component of the information environment[72]. Whilst the information environment is described in the doctrine as an element with 3 dimensions (physical, informational and cognitive), cyberspace is not described using the same architecture. It simply appears as a subset (which, though it is not explicit, might be assumed to follow the same outline), itself composed of a stack of "building blocks", which are networks, data and computers: "Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[73]. In this approach to cyberspace, we do not see the same level of importance given to information, and particularly to human beings (the cognitive dimension). Only the physical and technological dimensions appear to count. Unlike the information environment, where the approach is centered on humans, its definition cites individuals and organizations first: "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information"[74].

Thus, for its part, the information environment would be "human-centric", and cyberspace "technology-centric", unlike the "joint information environment", where the technological aspect wins out, looking at its definition: "The joint information environment framework is a set of mandatory standards, protocols, and principles that provides a secure and reliable shared IT infrastructure, enterprise services and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security, and improve IT efficiency. This framework enables DOD to acquire, operate, secure, and maintain IT capabilities to improve information sharing and better address cybersecurity"[75].

72 Page viii.
73 Page viii.
74 Page ix.
75 Page ix.

– JP 1-02, Department of Defense Dictionary of Military and Associated Terms, 8 November 2010 (As Amended Through 15 June 2015)[76]

The expression "information warfare" is no longer explicitly defined. A few terms on information warfare do remain, though, referring to the existence of centers and dedicated structures:

– AFIWC: Air Force Information Warfare Center;

– FIWC: Fleet Information Warfare Center;

– I2WD: Intelligence and Information Warfare Division (Army);

– IW-D: Defensive Information Warfare;

– IWSC: Information Warfare Support Center;

– LIWA: Land Information Warfare Activity;

– NIWA: Naval Information Warfare Activity;

– TWI: Office for Information Warfare Support (DIA).

Multiple expressions are given on the basis of "information operations", which refer primarily to the organization of the forces (command, troops) around these operations:

– information operations (defined on page 112)[77];

– information operations force (defined on page 112)[78];

76 http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

77 "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO. See also electronic warfare; military deception; operations security; military information support operations. (JP 3-13)".

78 "A force consisting of units, staff elements, individual military professionals in the Active and Reserve Components, and DOD civilian As Amended Through 15 June 2015 JP 1-02 113 employees who conduct or directly support the integration of information-related capabilities against adversaries and potential adversaries during military operations as well as those who train these professionals. Also called IO force. (DODD 3600.01)".

– information operations intelligence integration (defined on page 113)[79];

– DASD (S&IO): Deputy Assistant Secretary of Defense (Security and Information Operations);

– 1st IOC: 1st Information Operations Command (Land);

– G-7 Army component information operations staff officer; assistant chief of staff, information engagement; information operations staff officer (ARFOR);

– INFOCON: information operations condition;

– IOCB: information operations coordination board;

– IOII: information operations intelligence integration;

– IOT: information operations team;

– IOW: information operations wing;

– IOWG: information operations working group;

– IWC: information operations warfare commander.

Cyberspace, and the issues relating to it, for their part, are mentioned in the following items, in which we find the conventional dimensions of military cyberoperations – i.e. defensive and offensive – still pursuing an objective of "superiority" – an approach shared by all the domains (land, air, maritime and information). Various items refer to the organization of cyber forces (command, support, divisions, etc.):

– cybersecurity (defined on page 57)[80];

– cyberspace (defined on page 58)[81];

79 "The integration of intelligence disciplines and analytic methods to characterize and forecast, identify vulnerabilities".

80 "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire As Amended Through 15 June 2015 58 JP 1-02 communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (DODI 8500.01)".

– cyberspace operations (defined on page 58);[82]

– cyberspace superiority (defined on page 58);[83]

– defensive cyberspace operation response action (defined on page 63);[84]

– defensive cyberspace operations (defined on page 63);[85]

– offensive cyberspace operations (defined on page 174);[86]

– CDRUSCYBERCOM: Commander, United States Cyber Command;

– CNCI: Comprehensive National Cybersecurity Initiative;

– COMFLTCYBERCOM: Commander, Fleet Cyber Command;

– CSE: cyberspace support element;

– DC3: Department of Defense Cyber Crime Center;

– DCO-IDM: defensive cyberspace operations – internal defensive measures;

– DCO-RA: defensive cyberspace operations response actions;

– FLTCYBERCOM: Fleet Cyber Command (Navy);

---

81 "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (JP 3-12)".

82 "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-0)".

83 "The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary. (JP 3-12)".

84 "Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense cyberspace capabilities or other designated systems. Also called DCO-RA. (JP 3-12)".

85 "Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems. Also called DCO. (JP 3-12)".

86 "Cyberspace operations intended to project power by the application of force in or through cyberspace. Also called OCO. (JP 3-12)".

– JCC: Joint Cyberspace Center;

– NAVCYBERFOR: Navy Cyber Forces;

– NCIJTF-AG: National Cyber Investigative Joint Task Force-Analytical Group (DOD);

– NCRCG: National Cyber Response Coordination Group;

– NCSD: National Cyber Security Division (DHS);

– NMS-CO: National Military Strategy for Cyberspace Operations;

– USCYBERCOM: United States Cyber Command.

Thus, from all these documents, we see the emergence of three fields: information operations, information warfare (which manifests itself in what can be considered expressions or acronyms testifying to a still recent past), and cyber-operations. We also see the transition from information toward data, and an enduring obsession for the rollout of global solutions, with globality (systems, organization) being considered the "holy grail" which guarantees a real-time, complete and fair view of the situation, and thus ideal and guarantees the forces' action will be effective. Cyberspace has not yet managed to elevate itself to the rank of an entirely separate domain in its own right; it is still considered to be a subset. Indeed, rare are the texts which highlight its transversality. Instead, commentators prefer to focus on the fact that it is a component of something else – namely the information environment.

1.4. Important concepts and reflections

The very lively debate that has developed in the United States in the last 20 years involving the military, security experts, academics and other institutional and industry players has made it possible to produce a series of reflections on conflicts in the informational sphere or in the information age.

In the rest of this first chapter, some of the major themes will be discussed to either clarify concepts that have already been mentioned, or to introduce new ones that will be useful in the rest of the book.

1.4.1. *Information operations*

Information operations are the actions taken to affect the decision processes, information and information systems of the enemy, while defending our own information and information systems.

Commands use information operations to attack the decision processes, information and information systems of the enemy. Information operations are used to reach the C2 capabilities of the adversary; prevent his or her correct use of C2s, destroy, deteriorate, interrupt, deceive, exploit and influence them. In order to reach this goal, we must attempt to influence the perception that the enemy has of the situation. The objectives of information operations are to produce a disparity in the mind of enemy commands between reality and the perception they have, and to disrupt their capacity to exercise the C2. Information operations also affect the perception and attitudes of those located in the zone of operations: populations and civilian leaders.

Information operations can be offensive and defensive. Offensive information operations are the integrated use of methods and specific activities, supported by intelligence, to affect enemy decision-makers, or influence others. The desired effect is to destroy, deteriorate, disrupt, deceive, exploit and influence enemy functions. The ultimate targets are the leaders and human decision processes of the adversary or third parties found in the zone of operations.

Defensive information operations consist of the integration and coordination of policies and procedures, operations, personnel and technologies to protect and defend our own information and information systems. Defensive information operations ensure access to information (timely, precise, relevant and usable) while preventing the enemy from exploiting our information and information systems.

What activities make up information operations?

– military deception. Measures to deceive, mislead the enemy through manipulation, deterioration and tampering. The object is to

influence the understanding that the enemy may have of the situation and make him or her act against his or her own interests;

– counter-deception. These are the efforts to prohibit, neutralize or decrease the effects of hostile deception. Counter-deception supports offensive information operations by reducing the harmful effects of enemy deception;

– operations security prevents the enemy from accessing critical information that is vital to the success of military operations;

– physical security. Physical security protects from unauthorized access to installations, equipment and documents and safeguards and protects information and information systems;

– electronic warfare is a military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or to attack the enemy. It includes:

- electronic attack, to deteriorate, neutralize and destroy the enemy's electronic combat methods. These actions can include lethal attacks (missiles, directed energy weapons) and non-lethal attacks such as communications jamming,

- electronic protection, protecting the electromagnetic spectrum of our camp, protecting against electronic attacks (by radio silence and anti-jamming),

- electronic warfare support. To detect, identify, locate and exploit enemy signal transmitters, contributing to the understanding of the situation, the identification of targets and the evaluation of damages;

– information assurance protects and defends information systems. Threats are physical destruction, denial of service and malfunction. Assurance provides a greater degree of confidence in the possession of the following characteristics by information and information systems: availability, integrity, authentication, confidentiality, non-repudiation;

– physical destruction applies the force of the combat against targets with a connection to information operations. Targets include information systems, electronic warfare systems and control centers;

– PSYOPs are planned operations influencing behavior and actions of a foreign audience by circulating chosen information and precise indicators. PSYOPs are integrated to operations security, military deception, physical destruction and electronic warfare to create a perception of the reality supporting the objectives of allied forces. The expression "psychological operations" is replaced by "military information support operations" (MISOs) in JP 3-13.2, modified in December 2011.

– counter-propaganda includes activities directed at an enemy leading to PSYOPs against our camp. Preventive actions can be carried out consisting of increasing awareness, informing troops and population of the possibility and forms that hostile propaganda can take;

– counter-intelligence consists of identifying threats to security and knowing how to counter them. The threats are espionage, subversion and terrorism;

– CNAs are operations intended to interrupt or block operations, deteriorating and destroying information residing in computers or networks. Attacks can also target computers and networks themselves;

– Computer network defense (CND) consists of defending computers and other components interconnected in telecommunications networks against enemy CNAs. They include access controls, detection of malicious codes and intrusions;

– CNE, CAN and CNO are now dubbed cyber-operations – defensive and offensive;

– public affairs operations communicate information to critical audiences to influence their understanding and their perception of military operations. They influence populations by broadcasting information through the media;

– civil–military operations (CMO) apply civil affairs to military operations. These are activities that military commanders must conduct to establish, develop and influence relations between civilian authorities, government or the private sector and military forces. War no longer involves only the military. Links with civilian society are now very strong.

These various components of information operations (JP 3-13)[87], to which we must now add cyber-operations in accordance with military doctrine, are the subject of their own doctrines:

Component of information operations	Doctrinal document
Military deception (MILDEC)	JP 3-13.4, 26 January 2012[88]
Electronic warfare (EW)	JP 3-13.1, 8 February 2013[89]
Information assurance (IA)	JP 3-13, 20 November 2014
Psychological operations/military information support operations	JP 3-13.2, 7 January 2010, Incorporating Change 1, 20 December 2011[90]
Counter-propaganda	JP 3-13, 20 November 2014 JP 3-61, 25 August 2010[91]
Intelligence/Counter-intelligence	JP 2-0, 22 October 2013[92]
Cyberspace operations – defensive and offensive (CO)	JP 3-12(R), 3 February 2013[93]
Public affairs operations (PA)	JP 3-61, 25 August 2010[94]
Civil–military operations (CMO)	JP 3-57, 11 September 2013[95]

Table 1.2. *Components of information operations and their referential doctrinal documents*

87 Joint Chiefs of Staff, JP3-13, Information Operations, 27 November 2012, Incorporating change 1, 20 November 2014, 89 pages, Washington, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
88 Joint Chiefs of Staff, JP 3-13.4, Military Deception, 26 January 2012, Washington, 19 pages, http://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf.
89 Joint Chiefs of Staff, JP 3-13.1, Electronic Warfare, 8 February 2012, Washington, 144 pages, https://info.publicintelligence.net/JCS-EW.pdf.
90 Joint Chiefs of Staff, JP 3-13.2, Military Information Support Operations, 7 January 2010, 7 January 2010, Incorporating Change 1, 20 December 2011, 108 pages, Washington, https://www.pksoi.org/document_repository/Lessons/JP3_13_2_MISO_(20-Dec-2011)-LMS-1255.pdf.
91 Joint Chiefs of Staff, JP 3-61, Public Affairs, 25 August 2010, Washington, 113 pages, http://www.dtic.mil/doctrine/new_pubs/jp3_61.pdf.
92 Joint Chiefs of Staff, JP 2-0, Joint Intelligence, 22 October 2013, 144 pages, Washington, http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.
93 Joint Chiefs of Staff, JP 3-12(R), Cyberspace Operations, 5 February 2013, 70 pages, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.
94 Joint Chiefs of Staff, JP 3-61, Public Affairs, 25 August 2010, Washington, 113 pages, http://www.dtic.mil/doctrine/new_pubs/jp3_61.pdf.
95 JP 3-57, Civil-Military Operations, 11 September 2013, Washington, 173 pages, http://www.dtic.mil/doctrine/new_pubs/jp3_57.pdf.

The doctrine expressed by the latest version of JP 3-13 includes the following as components of information operations:

1) Strategic communication (SC);

2) Joint interagency coordination group;

3) PA;

4) CMO;

5) CO;

6) IA;

7) Space operations;

8) MISO;

9) Intelligence;

10) MILDEC;

11) OPSEC;

12) Special technical operations (STO);

13) Joint electromagnetic spectrum operations (JEMSO);

14) Key leader engagement.

These doctrines are expressed in proprietary documents for each force (Navy[96], Army[97], etc.). These versions sometimes introduce new distinctions, reflecting the different forces' visions. For instance, the

96 Department of the Navy, Navy Information Operations, NWP 3-13, February 2014, Office of the Chief of Naval Operations, Norfolk, VA, 68 pages, http://www.usna.edu/Training/_files/documents/References/3C%20MQS%20References/NWP%203-13%20IO.pdf.

97 FM 3-13, Inform and Influence Activities, FM 3-13, January 2013, Headquarters, Department of the Army, Washington, DC., 25 January 2013, http://armypubs. army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_13.pdf.

US Army's FM 3-13, of 25 January 2013[98], adopts other terminologies: it speaks of "Inform and Influence Activities (IIAs)" instead of information operations. These IIAs mobilize the following capacities:

– Public affairs;

– MISO;

– Combat camera;

– Soldier and leader engagement;

– Civil affairs operations;

– Civil and cultural considerations;

– Operations security;

– Military deception.

Note that there is not an exact intersection of the components as defined in JP 3-13. Also, cyber is only mentioned as a support for IIA. The document introduces the broad concept of "cyber electromagnetic activities" (CEMA), which include electronic warfare, cyberspace operations and electromagnetic spectrum management operations (FM 3-38).[99] Cyber-electromagnetic activities are those activities which take place in cyberspace and in the electromagnetic spectrum. IIAs and cyber-electromagnetic activities interact with one another, but they are nonetheless two distinct approaches, as stated by FM 3-13: IIAs target the whole of the information environment. The intersection between IIAs and cyber-electromagnetic activities is seen in the fact that CEMA help influence perceptions and decision-making. Cyber and electromagnetic activities, therefore, are of significance for IIAs when

98 FM 3-13, Inform and Influence Activities, FM 3-13, January 2013, Headquarters, Department of the Army, Washington, DC, 25 January 2013, 96 pages: http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_13.pdf.

99 US Army, FM 3-38, Cyber Electromagnetic Activities, February 2014, Headquarters, Department of the Army, 96 pages, Washington DC: http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf.

they facilitate action on the cognitive level. Here, electromagnetic activity appears as being distinct from cyber, but it is employed at the same level. The electromagnetic spectrum[100] (the arena for electronic warfare) and cyberspace (the theater of cyber-operations) are both components of the information environment. The electromagnetic spectrum and cyberspace also intersect one another.

The doctrines show the extent to which the information environment is complex, vast and requires the mobilization of multiple capacities, skills and resources. For example, the US Navy doctrine stipulates that the following should be mobilized in order to act in the information environment[101]:

– EW;

– Cyberspace operations;

– MISO;

– MILDEC;

– OPSEC;

– PA;

– CMO;

– Defense support to public diplomacy;

– Physical (lethal) attack;

– IA;

– Physical security;

– Combat camera (visual information) m. intelligence n. counterintelligence.

100 "The electromagnetic spectrum is the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands", US Army, FM 3-38, Cyber Electromagnetic Activities, February 2014, Headquarters, Department of the Army, 96 pages, Washington DC., page 1-5.
101 Page 3-1 of FM3-38.

The effect produced by such sets of strategies is that cyber is not placed higher than any other consideration, or any other object. It is merely one resource among various others in the information environment. However, its expansion, its transversality (clearly, cyber resources are used for MILDEC, PISO and CMO, for instance) mean, we feel, that it cannot be ranked at exactly the same level as the other components of information operations.

1.4.2. *Information superiority*

In a very general way, cyberspace is made up of computers, communication systems, networks, satellites, communication infrastructures and transport systems using information in its digital form (in cars, trains, airplanes, elevators, etc.), sound, voice, text and image data that circulates and is processed, systems that can be controlled remotely via a network, all control systems operating energy supplies, digital watches, video cameras, robots, as well as weapons, missiles, GPS systems, all technologies and communication tools (Wi-Fi, laser, modems, satellites, local networks, cell phones, fiber optic, computers, storage supports, fixed or mobile equipment, etc.).

This world of interconnections and interdependence, where information circulates from one medium to another and is processed, duplicated and stored, where tools communicate, where information technology becomes ubiquitous, constitutes the world of information, the information environment and cyberspace.

This environment, however, is reserved for a small group of the global population: those who can afford to pay for it. The distinction between those who can and those who cannot is fundamental because it divides the world in two. The digital divide progressively diminishes in very wealthy and developing countries where access to information technologies is increasingly possible. But it persists in the

gaps between wealthy and poor countries. The wealthiest countries on the planet are largely the beneficiaries of cyberspace.

The idea is mainly to acquire control of this sphere, an operation defined by the expression "info-dominance", because this control would be one of the major assets directing or deciding the outcome of crises, battles or conflicts. We often incorrectly present info-dominance as the ultimate goal of the great war powers (mainly the United States actually), thus confusing methods and objectives. Even though the fight for domination of the information sphere transforms information into a target, into a new, possibly virtual, front line to attack and defend, info-dominance still remains a method at the service of higher objectives: victory and political objectives. Info-dominance must not be an end in itself, but a step, a transition, an object of conquest, in times of peace or war, which once captured can contribute to paving the way to success.

The advantage of having information about an opponent is called "superiority of information". Superiority of information makes it possible to:

– obtain and process the best information;

– use this information more efficiently;

– see first, understand first, act first.

Superiority of information presumes:

– a capacity to collect, process and broadcast an uninterrupted data flow;

– being in a proactive situation. Being permanently in a state of reaction to operations carried out by the enemy prohibits information dominance.

The objective of superiority of information is to:

– affect the perceptions, attitudes, decisions and actions of the enemy;

– exploit capabilities by preventing the enemy from doing the same, as much as possible.

Superiority of information is characterized by:

– the central role that command must play, that must be able to direct operations, efficiently mobilizing methods, information systems and procedures. Information systems are a decision support tool;

– the series of methods that must be implemented: human, material and organizational methods;

– speed. Decisions must be taken quickly. Superiority of information confers the capacity of deciding and acting faster than the adversary. The objective is to lead the opponent at a pace at which he or she can no longer follow, that is detrimental to him or her, in order to keep him or her from being proactive. But the speed must not be detrimental to our own operations. Speed and obsession with "real time" are traps or illusions that command systems must be careful not to get into;

– the ephemera of the position of superiority. Nothing is definitive. The enemy also wants to have superiority of information. The situation permanently evolves; superiority is therefore transitory. Constant efforts must be made to retain this position;

– losing superiority of information means losing the initiative. From being proactive, we become reactive;

– aiming at the right objectives to acquire it:

- the enemy. We must understand his actions, prevent his or her access to, and exploitation of, his or her enemy's information, influence his or her perception, actions, his or her leaders, deteriorate and destroy his or her decision processes,

- non-combatants. We must influence them so that they support our camp and offer no resistance,

- our own camp. We must protect our own decision processes, information, information systems and provide correct information to commands.

To reach superiority of information we must act on ISR (intelligence–surveillance–reconnaissance), on information management (IM) and on information operations (IO). When the effects produced by ISR, IO and IM synchronization are greater than those of the enemy, superiority of information is then acquired.

In a situation of superiority of information, perception is close to reality. For the enemy, perception is different from reality.

The American military formalized the concept of superiority of information through their doctrines:

– in July 1996, the *Joint Vision 2010* (JV 2010)[102] was published, a founding text that provides a conceptual framework for American forces for the coming years;

– in May 1997, the Joint Warfighting Center published "Concept for Future Joint Operations. Expanding Joint Vision 2010". The report used the definition of superiority of information proposed in JV 2010: the capacity of collecting, processing and distributing an uninterrupted flow of information, while exploiting or paralyzing the capacity of the enemy to do the same;

– document Joint Pub. 3-13 from October 1998 recognizes the concept of superiority of information and its three components:

– activities that increase the capabilities of allied information systems, including the process of friendly decision support;

– intelligence and other activities linked to information providing information on friendly forces, enemies, or potential enemies in a timely, fair, precise and relevant manner;

– offensive and defensive information operations.

Information dominance appears as the capacity to revise strategies on the basis of a systematic analysis of the enemy and the capacity to identify his or her vulnerabilities and center of gravity.

102 Downloadable from http://www.dtic.mil/jv2010/jvpub.htm.

Info-dominance is achieved by transforming knowledge into capacity, identifying centers of gravity. The proliferation of information technologies has created the impression that information itself is a center of gravity. The objective of info-dominance is to have greater understanding, not total understanding.

Dominating information also means dominating the media and information in terms of news. Lessons from the past should serve as examples and be the basis for developing new theories and strategies in the field of communication. "From the perspective of the U.S. Military, television coverage of the Vietnam War had a detrimental impact on the conduct of that war; policies on television coverage of future conflicts should be revised so as to not repeat past mistakes"[103].

Having control of information does not spare the wealthier nations from significant setbacks. On 28 March 2003, the U.S. Air Force were given the mission of destroying elements of an Iraqi battery and rocket launcher to the north of Basra. There were different targets on the ground. Pilots received confirmation that there were no allied ground troops in the zone and launched their attack. They were quickly informed by ground troops that they had triggered a blue on blue incident. The pilots shot at the British, resulting in one dead and four wounded. The conversation was taped and a video (which is possibly a fake)[104] was quickly found on the Internet (notably on YouTube, with the title "Friendly fire – US Kills Brits in Iraq – Leaked video" or "The friendly-fire death of a British soldier in Iraq"). The event was widely covered in the media. Several articles were published on the Internet[105], as well as the dialog transcription between the two American pilots identified as Popov 35 and Popov 36, the latter being the shooter in question. Ground troops communicating with pilots

103 *Television coverage of the Vietnam War and its implications for future conflicts; Preamble;* Command and Staff College, US Marine Corps, 6 April 1984, http://www.globalsecurity.org/military/library/report/1984/HCD.htm.

104 The possibility of seeing fake videos remains great, over the Internet as well as in the media in general. We will not question here whether the video was a fake or real; we merely want to show that soldiers can find themselves in this or a similar scenario, and especially show that communication problems can occur in these environments.

105 http://www.tothecenter.com/news.php?readmore=961, http://www.guardian.co.uk/Iraq/Story/0,2006879,00.html.

were identified as “Manila Hotel”, “Manila34”, “Lightning34”, “Sky Chief” and “Costa58”[106].

The tape broadcast over the Internet lasted 15’24’’ (starting at 1336.30 GMT and ending at 1351.54 GMT). Aircrafts (A-10s) were at an altitude of 3,500 m. We should say that A-10s are not sophisticated fighter aircraft; they are, in fact, quite simple, designed for covering ground forces.

At 1336.57 GMT, Popov 36 reported that he thought he saw orange panels on the roof of the vehicles detected. This mark is usually installed on roofs of allied vehicles so they do not get confused with others. This identification requirement has long been a constant in the military (uniforms and colors made it possible to distinguish the different troops from afar. When commanders were in a high position and could observe the battle they needed clear indications to locate troop positioning and movement. When soldiers are in battle they need distinctive signals so they don’t shoot each other). Information technologies have now made this necessity redundant: an automated weapon system can detect if a person in the line of fire is a target or not, by detecting (for example) a signal sent back by that person’s equipment[107].

At 1337.16 GMT Popov 35 reiterated Popov 36’s report and received a confirmation from Manila Hotel: “Affirmative. No allied troops”. An exchange between the two pilots detecting the targets followed.

At 1338.49 GMT Popov 36 detected the vehicles and said: “it looks like they have orange panels on the roof”, Popov 35 then responded: “I’ve been told that there is nobody to the North”.

At 1339.09 GMT, for the third time in no more than 2 minutes, the pilots indicated having seen orange on the roof of the vehicles.

106 http://www.guardian.co.uk/Iraq/Story/0,2006914,00.html.
107 For more details on systems in development, see http://www.checkpoint-online.ch/Check Point/Materiel/Mat0039-DangerFeuAmi.html.

But, based on confirmations received, they formed another idea of what they were seeing on the ground: rocket launchers.

At 1342.09 GMT, Popov 36 fired, certain he was destroying rocket launchers. This was the attack in which the British soldier died. There were further firings at 1343.47 GMT.

At 1344.12 GMT, coming from Lightning 34, "[…] there are friendly troops in the zone[…]". Why did the information arrive two minutes after firing?

At 1344.39 GMT the pilots then requested information on the situation on the ground, which came back at 1347.09 GMT from Manila 34: "we have a first assessment showing one dead and one wounded".

We have here a combat situation during which one side fires on its own camp. This type of incident, friendly fire, has always existed during wars. Other incidents were recorded in Afghanistan (40 deaths attributed to friendly fire[108]) and in Iraq. Studies have attempted to evaluate the percentage of losses by friendly fire; between 12 and 15% of losses in all 20th Century wars. Will information technologies make it possible to decrease these numbers? What should we think about the 24% suggested for the Gulf War of 1991[109], even though that war was the advent of precision weapons!

What can seem surprising here is that, despite the so-called control of all dimensions of the combat, significant flaws remain. A number of consecutive errors led to bad, or even fatal, decision making:

– an intelligence flaw;

– the decision to shoot/not to shoot was not taken according to indications from the pilots and the doubt they expressed. Their first vision, which should have sounded alarms by creating doubt, was not confirmed by ground observation. It seems that the vision of the pilots

108 http://www.checkpoint-online.ch/CheckPoint/Materiel/Mat0039-DangerFeuAmi.html.
109 ibid.

was not taken into consideration in the decision. Their vision was then submitted to the influence of false information (there are no friendly troops in the zone). On this basis, the pilots formed a new vision that became conviction. Nothing, no mechanical or technical methods, or any procedure, make it possible for us to know what it was like in the pilots' shoes. Tactical decision support systems under stress seem to be nonexistent, inoperative. As the OODA loop accelerates, it seems that very little, if any, place is given to doubt, to questioning of information (although wrong to begin with), and disrupting the whole process;

– a problem of coordination/cooperation between American and British forces, on the ground and in the air, perhaps? Was there a failure of communication systems (GPS, radio)? Did the British convoy not announce its position?

– a failure or absence of a follow-up position or identification system in combat (IFF – identification friend or foe equipment – or still BFT – Blue Force Tracking – turned out to be inoperative in the present configuration).

Control of information is not only based on the dazzling increase of calculation capabilities, the multiplication of sensors and the increase in forces of physical destruction. The OODA loop accelerates, but in the heat of the action, there is no room for doubt to accelerate.

The decision to shoot relies here on the false information that there were no allied troops in the zone. Could we imagine the action being cancelled based on the doubts raised by the pilots?

The absence of information control by the authorities is also obvious when we see in how little time the video was released to the public. We must not forget that, beyond the fact that it had an impact on troop morale, friendly fire also has a political impact because it undermines the support of public opinion. For the public, friendly fire is the symbol of senseless death in war.

Blue on blue incidents, or friendly fire, are not specific to wars in the information age. Estimates of American losses (deaths) by the Pentagon in percentages[110], are:

– 16% during World War II;

– 14% in the Vietnam War;

– 23% in the Desert Storm operation (the much-talked-about precision fire!);

– 13% in the Afghanistan invasion.

Along the same lines of the "control of information/interpretation of information" problem, we can observe the controversy surrounding "The Apache Killing Video" (online on YouTube), or the video titled "Bombing Mistake" (2003 – Iraq) where we see an American aircraft bomb American troops mistaken for the enemy.

"The Apache Killing Video" was first broadcast on ABC TV to show how Americans treat insurgents. In the video, we see men going in and out of a truck seemingly transporting weapons in the night. We can distinguish forms and silhouettes and the scene is filmed by infrared camera from an Apache helicopter. The scene ends with the killing of Iraqi "insurgents", by firing from the helicopter. The video quickly raised questions: how could we be certain that the individuals filmed are really insurgents exchanging weapons, and not simply countrymen? The quality of the images does not make it possible to definitively lift doubt. One of the vehicles seen is a farm tractor. We then see a person picking up one or more long objects from the car. For the American military, the objects are missile launchers. It is impossible to dismiss the possibility that the objects may be simple farm tools or irrigation piping. The field of hypothesis is wide open.

What did Americans base their decision to open fire on? What was their perception of the scene? In doubt, are they given orders to fire? Was there an update of information from intelligence services?

110 Figures taken from http://www.answers.com/topic/friendly-fire.

The helicopter fires even though it is not threatened. Nothing in the men's attitude indicates a possible "attack" against the helicopter.

The helicopter dominates the situation; the men do not seem scared and do not make a hostile gesture.

What is, then, the reality of the situation? Was the information controlled by the helicopter pilots (compliance between information received from intelligence, C2 instructions, and correct interpretation of visual information received from their sensors)? Why and how did the video get to the Internet, to journalists? Is there not a process of suppressing sensitive information from the American military?

There are many who see this act as an assassination, a war crime according to the Geneva convention, article 3-1:1 of which states that: "persons not taking an active part in the hostilities, including members of the armed forces that have put down their weapons and those not able to fight […] will be treated humanely in all circumstances, with no distinction based on race, color, religion, faith, sex, […]".

These events demonstrate the gap that still exists between complete control of information and the actual capacities of the best equipped military. The idea of a zero death war must also be forever erased from our minds. Zero deaths for whom? The Americans wished to shield their troops, but certainly not those of the enemy. It is illusory, and naïve, to believe in the possibility of a zero death war when we deploy troops, and especially weapon systems, on the scale of what has been done in the more recent wars. "Zero death" is dead. There are precise target shootings. There is collateral damage (enemy civilian), errors (firing against our own camp), the impossibility of controlling all movements and all human decisions in real time in the heat of action. Is there today a flawless automated decision system, able to distinguish an enemy target from an ally, able to decide to shoot, even to shoot alone, with an error margin close to 0%? No. Man is, and will remain, at the core of the process of the OODA loop. And man's intervention is extremely complex to model and to control. The combat situation, or simply the context of war, even if there is no direct threat on the life of a man, influences his behavior, his psychology. Why did the helicopter pilot make the decision to fire?

Was he certain he was faced with a target, i.e. an enemy representing immediate danger? What, in the scene that he could not directly see, except through a screen, sensors and data processing systems, influenced his reasoning to the point where he thought "I must shoot"? Was it the immediate situation, or the immediate situation taken from all the images built prior to the situation, his conscious or subconscious modeled in a more general context of the war? In this environment, the soldier is perpetually surrounded by threats, real or shaped (by propaganda internal to the military, by the influence of other soldiers or by the media), including the threat from his own camp (remember the percentage of losses attributed to friendly fire in the Gulf War: 24% or approximately one death in four)[111].

The soldier does not see the scene as we do, sitting safely in front of our computer. The error we make when trying to rectify this type of incident is our belief in the existence of computer systems, making the soldier out to be a 21st Century cyber warrior with a precise and infallible aim. The United States is working toward that goal but the dream is still beyond reach. Even if technology enables us to fire long range without seeing or being seen because of the existence of information technology in weapon systems, it seems painfully obvious that not everything is possible. Research into the field of man–machine and man–man interaction via machines, and into interaction in a problem scenario and cognitive systems, is a priority. We must understand how man thinks and acts according to his environment if technology wants to be able to offer him the tools to assist him, or even replace him, in making decisions and taking action.

It takes a long time for man to make decisions in a situation of war, in stressful situations or in emergencies – all disturbing contexts. The presence of information can be valuable in making decisions. But the multiplication of data sources, and the increase in the volume of information that could be contradictory, will not necessarily alleviate man's stress nor diminish the number of errors. In 1998, the *USS Vincennes* shot down an Iranian jetliner, mistaking the Airbus A-300

111 http://www.checkpoint-online.ch/CheckPoint/Materiel/Mat0039-DangerFeuAmi.html.

for an F-14 fighter, killing 290 people. Will ICTs make these tragic errors of decision impossible in the future?

1.4.3. *The "value" of information*

Information is a series of facts, data and instructions available in any medium, in any format. It is the meaning that man gives data through known conventions used in their representation. The same information can convey different messages and send mixed signals to recipients and users of this information, including the intelligence community[112].

Information has always had a major role in human societies. But today, information has a new and dominating status, stimulating almost all aspects of social life and modern war. The importance of information in strategy, tactics and operations has long been emphasized in the context of conflicts, notably by the Chinese, Sun Tzu: "If you know your enemy, you should not fear the outcome of a battle". Information is a strategic resource and weapon. Information also has value.

Information, information systems and information-based processes used by the military must be the subject of protection proportional to the value of the information and associated risks. The value of information can change, however, according to objectives in times of peace, crisis, conflict or post-conflict, as well as during the different phases of an operation. This link between information and security value makes any information a potential object to protect. Information may have no value today but tomorrow it will have value if the context changes. In that case, what must be protected? And when can we define that information must be "protected"?

In order to have value, to be processed, analyzed and help in a decision, information must not have been subject to distortion or carry risks. Criteria for quality include:

112 JP 3-13, 1998 version.

– precision and accuracy: the information reflects the situation;

– opportunity: the information has not been surpassed by events;

– usefulness: the information is easily understood and displayed in a format that makes sense immediately;

– completeness: the information must contain all the necessary elements;

– precision: a level of detail is required;

– assurance: we must be certain that the information is not corrupt, fake, deteriorated and that it is accurate.

Several categories of information can be distinguished:

– information that is required, where needs are clearly identified by commanders; facts, evaluations and hypotheses;

– information that is important but the need has not been specifically expressed by commanders (implicit needs);

– information that commanders need but do not possess;

– information that the commander does not have and knows nothing about;

– information that is not useful, that commanders do not need to know but that they are given. Too much information of this nature can saturate the decision process. The information must therefore be filtered, which is the role of a good information management system.

Information can also be classified into:

– facts: the information that we want to learn from an accurate and confirmed source;

– evaluations and hypotheses: this is the information that we want to know but that we cannot have with certainty.

Finally, all this information must be managed. This is the role reserved to information management systems responsible for providing relevant information to the right person, at the right time, in a usable form, in order to facilitate understanding and decision making

(see document FM 6-0). Information management must ensure information circulation through the different communication networks, add meaning to information, rely on information systems (equipment and infrastructures that collect, process, store, display and broadcast information, and are an integral part of C2 systems), and ensure reliable and relevant information. Four rules must be retained:

– information that does not arrive on time and unusable information have the same effect as an absence of information;

– incomplete or inaccurate information is more important than the absence of total information;

– not relevant, inaccurate and imprecise information is worse than a total absence of information;

– relevant information must be precise, appropriate, useful and usable, complete and reliable. But relevant information at moment T can lose its quality at T+1. Relevant information is perishable.

A conflict (information warfare) confers three important characteristics to information:

– it is desirable: it is the information that we must acquire (databases, satellite images, confidential information, access codes and knowledge);

– it is vulnerable: software, databases, information systems, memory, sites, networks, all information vectors/supports, are vulnerable, can be victims of attacks, distorted, deteriorated, damaged, or even victims of their own deficiencies. In fact, the information itself is vulnerable;

– it is frightening: viruses, rumors, anything where propagation is favorable to one camp and harmful to the other. For example, instead of the sometimes dangerous lie that can come back to bite its users, we prefer truth, more efficient, but filtered, sorted in order to only broadcast information that can have a positive impact on our troops and public opinion, and doing the opposite with the adversary's public opinion.

Efficient information is information with a value that is based on its distribution and not its truthfulness. Information is efficient if it finds listeners, receivers and believers adopting the proposed point of view.

1.4.4. *Information system*

An "information system" is a group of infrastructures, organizations, people and components that collect, process, store, transmit, display, broadcast and act on information. Information systems also include information-based processes[113].

An information system is made up of integrated doctrines, procedures, organizational structures, equipment, methods and communication systems designed to help in the execution of C2 during military operations, by collecting, processing, analyzing, archiving and broadcasting information[114]. Seven components form the basic functions of information systems:

– sensors to capture data;

– processors that filter and organize data into information;

– receivers: who uses them? They can be automated weapon systems, decision support systems or decision makers themselves;

– databases, scheduling and research for stored information, regularly updated and secured against corruption or theft;

– transmitters for information distribution;

– rules defining operations and system structures;

– synergy, the most important component, ensuring that the system operates better than the sum of each of its parts, for real added value.

113 JP 3-13, 1998 version.
114 Information Operations and the Conduct of Land Warfare, *Military Review*, vol. 78, no. 5, pp. 4–17, September–November 1998.

Information warfare consists of attacking these components and defending ours.

"Information-based processes" are the "processes that collect, analyze and distribute information in any medium or form"[115]. These processes can be present in all facets of military operations (combat, combat support, etc.) and in the elements of national power. They are included in all systems and components requiring facts, data and instructions, from strategic reconnaissance systems to important enemy decision makers, etc.

1.4.5. *Command and control warfare: C2W*

The role of command and control (C2) is to "exert authority and direction by designated command on forces connected to it, in the accomplishment of a mission"[116]. C2 must plan, direct, coordinate and control forces and operations in the accomplishment of the mission.

Communications systems, surveillance systems and computer networks constitute C2 systems, enabling commanders to have a global vision of the battlefield and exert their authority on the methods under their control to reach their objectives. C2 systems are based on the security of communications systems. The objective of C2 systems is to promote a united effort, with centralized direction and decentralized command execution.

"Command and control warfare" (C2W) is the integrated use of OPSEC, military deception, PSYOPS, electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information, to influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. C2W is an application of information operations in military operations. C2W is both offensive and defensive.

115 JP 3-13 1998 version.
116 JP 3-13 1998 version.

The OODA loop is a paradigm useful in the analysis of C2-type decision-making and activity planning. The C2W concept represents offensive information operations serving to disrupt the OODA loop of the enemy[117].

Generally, the concept ties in offensive and defensive information operations. In a note in January 1995, the Marine Corps defined C2W as any action taken by military commanders to carry out the practical effects of information warfare on the battlefield[118]. This approach includes actions blocking the enemy C2 while protecting our own C2. C2W integrates the physical destruction of the enemy's C2 targets, EW, military deception, PSYOPS and OPSEC.

The C2 process can be perceived as a fundamental universal human activity and would constitute, according to some authors [SHA 98], the battlefield of information warfare. The object of information warfare in C2 is to make the allied decision process more efficient, and enemy decision process more difficult and uncertain. C2 warfare consists of monitoring the enemy and our own troops and resources, planning and re-planning EW scenarios, evaluating alert signals and evaluating damages resulting from attacks, controlling the situation of a specific conflict, choosing methods of operation, facilitating execution, evaluation and control while maintaining military methods, by reconstituting and redirecting forces, and finally negotiating with the enemy to end the conflict. C2 functions are enabled by communications and intelligence systems. C3I (command, control, communication and intelligence) is the most essential component of information warfare.

A doctrinal text on C2W is used as a reference: JP 3-13-1: Joint Doctrine for Command and Control Warfare (C2W).

117 For a definition of the OODA loop, see section 1.3.7.
118 Instruction 3430.26. Department of the Navy. Washington DC 20350-2000. OPNAVINST 3430.26, No. 6, 18 January 1995.

1.4.6. *Effect-based operations (EBOs)*

To see accurately in order to touch accurately, to see well, better, faster, while remaining invisible to the enemy; it is the combination of these factors that made it possible for the US Air Force to become a decisive instrument.

Because of the influence of Boyd[119] and the theory of emerging systems, the Air Force developed a method based on a systems approach that emphasizes the effects of attacks on the enemy. It is no longer enough to destroy enemy forces, instead we must win by aiming at and hitting targets liable to have the most impact (through chain reactions), like enemy troops, the organization, the decision-making process and logistics. In this way, "small" attacks, i.e. precision hits, can have very strong effects on a whole system. The reason is the dynamics inherent to large systems, amplifying the results of an attack. In economics, we would speak of a good return on investment (ROI).

Although the great powers developed the principle of EBOs, the Iraqis, for example, also used it as their own and organized it so that they could put in practice the principle of EBO with small guerrilla cells. These cells are practically undetectable and very difficult to neutralize.

A viral computer attack can also be interesting as an EBO. Launching an attack can be simple, and the attack might not be severe enough destroy; indeed, it might not be intended to destroy but rather to cause secondary damage in series (paralyzing a computer system, for example, which paralyzes the operations of a company, blocking its economic activity and having consequences on relations with partners and clients). But an uncontrolled viral attack can sometimes lead you to shoot yourself in the foot; the military would speak of "blue on blue" or "friendly fire".

119 John R. Boyd, *Destruction and Creation*. p. 8, 3 September 1976, http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf.

1.4.7. *The OODA loop*

Colonel John Richard Boyd (1927– 1997), pilot in the US Air Force, proposed a model for the decision cycle, based on his experience in combat. The concept that he proposed is known as the "OODA loop".

This concept is an abstraction describing the sequence of events as they must occur in any military battle:

– O = Observation. The enemy must be observed to gain information;

– O = Orientation. The attacker must put himself or herself in the context, in situation;

– D = Decision. The attacker must then decide; and finally;

– A = Action. The attacker must act.

From a practical standpoint, what confers the advantage over the enemy in a battle is the capacity to always be one step ahead of the enemy, to impose the pace of operations, maintaining initiative, forcing the enemy into a reactive state by prohibiting any initiative, any preemptive capacity.

We must always be ahead in this loop in relation to our enemy; the one who goes around the loop faster has an operational advantage leading him or her to victory.

Superiority of information enables us to get round the loop faster. Network centric warfare (NCW) systems also help us take advantage of this loop. Accelerating the loop means accelerating its four elements:

– O–O–D: these phases are centered on information. We must obtain the information, distribute it, analyze it and understand it. The network operation accelerates phases O–O and facilitates phase D;

– phase A (Action) is centered on movement.

This concept of a loop is used in the military field but has also been used in other fields (such as, for example, in economics and finance) where the capacity for quick decision making must confer a decisive advantage over an adversary/competitor.

In the early 1990s, planning combat objectives required approximately 24 hours. Today, we can consider reaction times of approximately 30 minutes.

1.4.8. *RMA*

The acronym RMA stands for "revolution in military affairs".

Does the transformation that global armed forces go through only involve new technologies or does it also lead to deeper conceptual or doctrinal changes?

Early in the 1980s, a part of the Red Army led by Marshall Nikolai Orgakov wondered about the transformation of war. He predicted that the rapid changes in information technologies and high-tech weapons such as the ones used by NATO would lead to radical changes in the way to conduct a war. Orgakov spoke of a "technological military revolution". His predictions turned out to be true with the United States' victories in the Gulf War (1991) and Kosovo (1999).

Different points of view on RMA divide the comments on it as a concept:

– RMA supporters maintain that the transformation of weapons, military technology, organization and doctrines greatly reinforce the efficiency of the military;

– those from the school of asymmetric conflicts focus on the importance of asymmetrical conflicts such as guerilla and counter-terrorism. They maintain that the major threats in the post Cold War period remain unconventional forces. The United States, in 1990–1991, demonstrated the technological superiority of conventional Western forces. Adversaries have no choice but to attack the weak elements of their Western enemies, who are technologically more advanced, by

using terrorism, weapons of mass destruction and, more probably, bypass strategies and tactics. There really was a technological revolution, and the introduction of these revolutionary technologies considerably reinforced the military, giving it new superiority in weapons and forcing adversaries to choose new solutions;

– sceptics doubt that current military progress represents a revolutionary change. They speak of evolution instead of revolution. If there must be revolution in military affairs, it will be done through a revolution of doctrine, since the technological revolution is not able to trigger this fundamental revolution. Sceptics prefer to speak of "transformation" instead of "revolution" in military affairs.

But the question has been raised and remains, involving the possibility of there being a revolution in military affairs. There are two opposite points of view:

– New information and communication technologies (NICTs) constitute a technological revolution. Their introduction in the military puts everything into question: organization, tactics, strategies and doctrines. A revolution in the field of information is at the basis of a real revolution in military affairs;

– NICTs are undeniably a technological revolution but their introduction in the military is perceived merely as the introduction of new methods, which will not revolutionize the military mind. NICTs are then considered as a simple force multiplier, i.e. adding methods to the ones already in place, adding methods in a familiar environment for the military, forcing them to adapt to defined models such as speed, precision and lethality. This (simplistic?) vision is not synonymous with a profound change in military outlook.

One response, with a play on words, could be that there is clearly a revolution in military affairs (the introduction of new technologies) but there is no revolution of the military affairs.

Regardless of the doctrinal considerations of the military toward the introduction of NICTs within their core, and the more-or-less advanced development of war tactics and strategies of information, the

introduction of these technologies has had an obvious impact on the military all over the world:

– the militaries of wealthy and industrialized countries have thrown themselves into a race for high-tech, software-based, weapons. The technology continues to evolve, and keeping up-to-date with developments forces significant investments to acquire them and for R&D. Importing foreign technologies may seem like a good alternative, but remains expensive;

– the most powerful NICTs are mostly developed by the private sector, and what's more, these developments are not *a priori* meant for the military. Developing and strengthening cooperation between private industries and the military sector has become one of the most relevant issues of national security and defence policies not only in the USA but also all over the industrialized world: first, because information technologies can be dual, and work with civilian as well as military applications; and second because, if the military wants to acquire superiority of information, it must not settle for off-the-shelf products, black boxes that will be integrated with current systems. Whoever has technological control can claim control of informational space.

1.4.9. *C4ISR*

C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems are the networking computer resources which make communication possible between target acquisition systems and weapons systems.

They provide support for NCW, a way to fight a war by exploiting the capabilities of information systems and networks. They make it possible to coordinate and execute complex, joint operations with precision, accuracy and speed. C4ISR systems are a series of military functions for coordinating operations. C4ISR represents the infrastructure or the procedures used. These systems are implemented through an architecture called DODAF (DoD Architectural Framework) that must link the different military wings of a country together, and the military with allied forces (joint or coalition forces). France does

not use the term C4ISR but instead uses *bulle opérationnelle aéroterrestre* which, in English, translates as "air and land operations bubble".

1.4.10. *Network Centric Warfare (NCW)*

NCW was defined by Cebrowski in 1998. The concept was placed at the core of the Transformation Program applied to the American military initiated by Donald Rumsfeld.

The principle is based on geographically dispersed units with real time information, interconnecting and collaborating with each other, accessing, sharing and protecting information. ICTs help in making small units function in networks, interconnecting them and giving them ways to communicate and coordinate. This form of organization can be compared to a swarm of bees.

This theory also brings up the principle of adopting civilian technologies and introducing dual technologies by the military. The introduction of networking techniques in combat systems is the military equivalent to the digitization, computerization and networking of civilian systems which took place from the middle of the 1980; i.e. it is a radical and profound change, a major evolution.

Networking has several objectives, constraints and characteristics:

– it must accelerate the cycles of engagement;

– it must accelerate the operation's pace by accelerating the O–O (Observation–Orientation) phases of the OODA loop;

– it must be done with wireless technologies which constitute the core of the NCW architecture, because platforms, units and people are mobile;

– combat platforms must be digitized to be able to transmit information from one platform to the other.

Technical problems generally dominate the debate on NCW to the detriment of doctrinal or strategic aspects:

– how can we secure communications to avoid the information from being intercepted? This is the role of cryptography. We must also make sure that transmissions are undetectable;

– communications must be robust and must be resistant to jamming and to weather conditions;

– the more secure and robust a transmission must be, the more throughput intensive it becomes. Transmissions must, however, remain quick;

– messages and signals must be correctly routed;

– communication between platforms must be ensured through total interoperability of the multiple protocols used by the different aviation, marine and ground forces communication systems.

1.4.11. *ISR: intelligence, surveillance, reconnaissance*

ISR is fundamental in the process of acquisition of superiority of information. In order to be efficient, ISR must be integrated. There are a large number of data sources, and common and coordinated mechanisms must therefore be in place. The role of ISR is to produce intelligence on the enemy and the environment.

Intelligence is the product of the collection, processing, integration, analysis, evaluation and interpretation of available information involving foreign countries. It is the knowledge that we have of an adversary, obtained from observation, research, analysis and understanding. Analysis is the fusion of information and intelligence from each discipline within ISR. It is distributed and is collaborative. Intelligence must be shared, from the national to the tactical level. It provides a critical support for all operations, obviously including information operations. It helps in the planning, decision and identification of targets.

Reconnaissance is the collection of information and makes it possible to validate current intelligence or predictions.

Reconnaissance is a mission carried out to obtain information on the activities and resources of an enemy or a potential enemy, as well as on the weather, hydrographic and geographic conditions of a specific area through visual observations or other detection methods. It is incorporated in the conduct of all operations, including information operations. It makes it possible to collect information that cannot be accessed through other methods. Reconnaissance units are also sent on missions before operations, but generally do not fight. However, an aggressive reconnaissance can mislead the enemy, make him believe that operations are launched and thus show his or her hand too soon.

Surveillance is the systematic observation of the airspace, ground and submarine/underground space, people and things, through visual, oral, electronic and photographic methods.

1.4.12. *Cyberwar*

In his article "Cybernetic Wars", published in the American journal *Omni* in May 1979, Jonathan V. Post discusses the role of the computer in warfare[120]. In his view, this technological evolution marked the beginning of a new era – the era of the Third World War, of cybernetic war, characterized by the infiltration of computer technology into all modern weapons systems. This cybernetic war is the fusion of computer technology and all of the scientific advances (robotics, lasers, missiles, smart bombs, etc.), employed for the purposes of war. It was John Arquilla and David Ronfeldt who first truly introduced the modern view of cyberwar, in 1993 in their article "Cyberwar is coming!"[121].

The concept, which had been used relatively little over the past decade, experienced a revival essentially at the end of the 2000s

120 Jonathan V. Post, "Cybernetic Wars", *Revue Omni*, 1979 [http://archive.org/stream/ omni-magazine-1979-05/OMNI_1979_05_djvu.txt].
121 John Arquilla, David Ronfeldt, "Cyberwar is coming!", *Comparative Strategy*, vol. 12, no. 2, pp. 141–165, 1993.

(notably in the wake of the cyber attacks that hit Estonia in 2007), in the debates concerning modernization of warfare and the evolution of the modes of conflict between actors on the international stage. During this period (1993 to the present day), various definitions of cyber warfare were formulated. The concept of cyber warfare, though, goes beyond the mere process of computerization of armies and weapons systems. It suggests that the new information age and the networked society have given rise to a new category of war, which takes place in a planet-wide battlefield – cyberspace – and goes beyond the conventional context of inter-State armed conflict. This new form of warfare can either be positive (a new category of warfare which is less costly, cleaner and less risky[122], and which enables strength to be projected, in a different way, to any point on the globe), or negative (cyberwar would be the greatest threat that nations have ever faced[123]). Introducing new modes in the art of war, or a new category of war, cyber warfare is supposed to represent a breakthrough in the evolution of conflicts[124], contribute to the evolution of international relations by altering the ratios of strength between States in a way never before seen, and giving non-State and/or asymmetrical actors new means of action allowing them to defy the power of States and to play a real role on the international scene.

Cyber warfare is not defined in the documents of the US military doctrine[125], which adopt other terminologies: cyberspace, a

122 Myriam Dunn Cavelty, "Cyberwar: concepts, status quo, and limitations", *CSS Analysis in Security Policy*, no. 71, p. 3, April 2010, [http://bsu.ase.ro/oldbsu/anexe/lectures2010/CSS_Analysis_71.pdf].

123 Lionel D. Alford Jr,, "Cyber warfare: a new doctrine and taxonomy", *The Journal of Defense Software Engineering*, pp. 27-30, April 2001, [http://www.crosstalkonline.org/storage/issue-archives/2001/200104/200104-Alford.pdf].

124 Richard A. Clarke, Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, United States, p. 320, 2010, Trefor Moss, Is Cyber War the New Cold War?, *The Diplomat*, 19 April 2013: http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/.

125 Joint Chiefs of Staff, JP 3-12, Cyberspace Operations, 5 February 2013, Washington, 70 pages, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf.

subcomponent of the information environment, is the space in which defensive and offensive cyber-operations take place (these terms substitute the previous "computer network defense" and "computer network attack"), with the objective being to achieve superiority in that space (the documents speak of "cyberspace superiority" and "dominance in cyberspace") – approaches which are largely inspired by or inherited from the formulations and considerations adopted for the other environments: particularly the information environment (the place of information operations). The concept is still used, though, in the literature of the US land army[126]. This document considers cyber warfare as a composite brick, which is technically structured around *cyber operations* (CyberOps), *cyber network operations* (CyNetOps), *cyber support* (CyberSpt) and *cyber situational Awareness* (CyberSA). The term *cyberwar* in the text is the contraction of *cyberspace warfare*.

Mention is also made of the term on the official Website of the US Army Cyber Command: "Cyber Command is composed of a professional team of elite warriors defending Army networks […] The cyber war fighting requires impact, integration, risk, and knowing ourselves, the enemy, and the cyber terrain"[127]. The US Secretary of Defense also employs the concept of cyber warfare in his speeches[128]. NATO, in its Research Papers, in November 2010 published an article entitled "Cyber war and cyber power"[129], though pointing out that the Organization does not refer to cyber warfare but instead prefers to speak of "cyberdefense". Cyber warfare can sometimes be understood

126 *Cyberspace Operations. Concept Capability Plan 2016-2028,* The United States' Army, TRADOC pamphlet 525-7-8, 22 February 2010.
127 [http://www.arcyber.army.mil/org-arcyber.html].
128 In this regard, see the chapter of that thesis devoted to the study of discourse on cyber warfare.
129 Jeffrey Hunker, *Cyber War and Cyber Power, Issues for NATO Doctrine,* NATO Research Paper, Rome, no. 62, p. 12, November 2010, [http://www.ndc.nato.int/download/downloads.php?icode=230].

as a synonym for information warfare[130], or as a constitutive element of information warfare, a subset of it. Cyber warfare is "combat in the virtual domain"[131], or "cyberspace"[132], which itself is a subset of the information environment.

Essential criteria of the definition	Definitions	Author
Focus on the theoretical and doctrinal framework		
I - Reference to Clausewitz: a Clausewitzian conflict, or indeed a non-Clausewitzian one	"Cyberwar should be the use of cyber warfare[133] (that is, techniques used to usurp the control of computers from their authorized users), in pursuit of politico-military aims (i.e., something that Clausewitz would recognize)."	Martin Libicki, 2013[134]
	According to Thomas Rid, cyber warfare should to conform to the Clausewitzian view of war: any act of war must potentially be lethal, must be an instrument (weapon, attack, threat), in the service of politics (imposing one's will). This, from his point of view, can never actually happen (the main difference lies in the non-	Thomas Rid, 2013[136]

130 "Guerre de l'information : mise en place d'unités spéciales dans divers pays", *in Sûreté de l'information, situation en Suisse et sur le plan international*, p. 16 of MELANI report, Switzerland, January-June 2009.

131 Libicki Martin C., *What is Information Warfare?,* Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS), Washington, National Defense University, p. 110, August 1995.

132 S.S. Azarov, A.G. Dodonov, "Instrumental Corrections for a Definition of Cyberwar", in Carvalho Fernando Durate, Mateus da Silva Eduardo (eds), *Cyberwar-Netwar*, IOS Press, p. 159, 2006.

133 Martin Libicki draws the distinction between "cyberwar" and "cyber warfare", which is combat in cyberspace, using cyberspace.

134 Interview of Martin Libicki (RAND Corporation) by Daniel Ventre, April 2013: http://www.chaire-cyber.fr/IMG/pdf/article_3_1_-_chaire_cyberdefense_2_.pdf

	lethality of cyber-operations). "No known cyber attack has yet satisfied the Clausewitzian definition of the act of war"[135].	
	Cyberwar[137] "is a situation of conflict between at least two political actors characterized by the deliberately-hostile and costly use of cyber attacks, against the critical civil or military infrastructure, with a coercive intention, with the aim of obtaining political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's defense capability, or ability to respond in kind or by conventional force, or against civilian or military targets with strategic objectives"[138] . This definition breaks away from the majority of the literature, drawing inspiration less from the partial lessons and quotes from Sun Tzu and more from Clausewitzian conceptualizations of war.	Adam P. Liff, 2012[139]
	Cyberspace is not a space of combat. With this approach, cyber warfare loses its whole foundation, and a form of ware without a theater of combat is no longer explicitly Clausewitzian.	Martin Libicki, 2012[140]
	Cyber warfare is a form of secret war (thus, it differs from Clausewitzian war, which is open, with adversaries facing each other and knowing	Martin Libicki, 2011[141]

136 Thomas Rid, *Cyber War Will Not Take Place*, London, Hurst & Co Publishers Ltd, p. 256, April 2013.

135 Thomas Rid, *Cyberwar and Peace, Hacking can Reduce Real-world Violence,* Foreign Affairs Website, November-December 2013: http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace].

137 "Cyber warfare" in the text, but "cyberwar" in the title.

138 Cyber warfare is "a state of conflict between two or more political actors characterized by the deliberate hostile and cost-inducing use of CNA against an adversary's critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purpose".

139 Adam P. Liff, "Cyberwar: a new "absolute weapon"? The proliferation of cyber warfare capabilities and interstate war", *Journal of Strategic Studies*, 35/3, pp.401-428, June 2012, http://indianstrategicknowledgeonline.com/web/Proliferation% 20of %20Cyberwarfare%20Capabilities%20and%20Interstate%20War.pdf.

140 Martin Libicki, "Why cyberspace is not a warfighting domain, *A Journal of Law and Policy for the Information Society*, pp. 325-340, Fall 2012.

	one another).	
II - Distinguishing between a new appearance of war and a new category of war	Cyber warfare is a state of open armed conflict between nations, States or parties which is in relation with, or involves, computers or networks of computers. Obviously, any modern contemporary army uses computer technologies in one way or another. Any war today, therefore, could qualify as cyberwar. In addition, we should no longer speak of cyberwar, but rather of cyber conflicts, to denote the computer-based aspects of war. Cyberwar suggests the existence of a new, distinct form of war.	Kai Denker, 2011[142]
III - Cyberwar is a dimension of conventional war	Cyber warfare is the use of computers or digital means by a government or with explicit knowledge of or approval of that government against another State, or private property within another State including: intentional access, interception of data or damage to digital and digitally controlled infrastructure. And production and distribution of devices which can be used to subvert domestic activity.	UN Security Council, 2011[143]
	Cyberwar on its own cannot exist. It is the extension of a conventional war, or is part of a conventional war. "A pure cyberwar – in which only cyber-weapons are used – is improbable. Future wars and the skirmishes which precede them will be a mixture of conventional or kinetic weapons and cyber-weapons, serving to disrupt or to increase the user's strength."	P. Sommer, I. Brown, 2011[144]
	Cyberwar is the cybernetic dimension of armed conflict. "Cyberwar is the technical dimension of information warfare; the use of cybernetic capabilities to carry out aggressive operations in cyberspace, against military targets, against a State or its society; a typical war where at least one of the	Éric Filiol, 2010[146]

141 Martin Libicki, "Sub rosa cyber war", in Christian Czosseck, Kenneth Geers, *Cryptology and Information Security Series*, vol. 3, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam NL (IOS Press), pp. 53-65, 2011.
142 Kai Denker, *Cyber War and Cyber Crime – Implications of a Vague Difference*, Darmstad University, p. 5, 8 April 2011, [http://www.inter-disciplinary.net/wp-content/uploads/2011/04/kaiwpaper.pdf.
143 United Nations Security Council, Resolution 1113 (2011), 5 March 2011, 1 page.
144 Peter Sommer, Ian Brown, Reducing Systemic Cybersecurity Risk, report for the OECD, Information Systems and Innovation Group, London, London School of Economics, p. 121, 14 January 2011.

	components, in the realization, motivations and tools (weapons in the broadest sense of the word), is based on the computerized or digital field".[145]	
	"A conflict between two or more States, intended to damage the systems, processes and computer resources, and to attach the political, economic and social systems and to indoctrinate the masses to destabilize the society and the State, but also to force it to take decisions that favor the interests of an enemy party."	Shanghai Cooperation Organization, 2009.[147]
	There can be no cyberwar without war.	Bruce Schneier, 2008[148]
	"A conflict which employs hostile, illegal transactions, or attacks against computers and networks, in order to try to disturb communications and other parts of the infrastructure."	Clay Wilson[149]
	Cyberwar does not completely replace war: "It supplements it, it supports it, reorganizes it. The cyberwarrior cannot replace the traditional warrior."	Laurent Murawiec, 1999[150]
IV - A general concept, cyberwar, and various subdivision	Operational cyberwar (support function, as was aerial war): acting against military targets during strategic cyberwar: cyber attacks against adversarial/enemy civil infrastructures	Martin Libicki, 2009[151]
	Limited cyberwar, where the information	Timothy

146 *Ibid.*

145 Éric Filiol, "Aspects opérationnels d'une cyberattaque : renseignement, planification et conduite", in Ventre Daniel (ed.), *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*, Paris, Éditions Hermès Lavoisier, p. 319, 2009.

147 Shanghai Cooperation Organization, Appendix I to the agreement between the governments and the Member States of the Shanghai Cooperation Organization over the question of cooperation for international security of information, 16 June 2009.

148 Bruce Schneier, "For it to be cyberwar, it must first be war", cited in "Marching off to Cyberwar", *The Economist*, 4 December 2008, www.economist.com/node/12673385.

149 Clay Wilson, Information Operations and Cyberwar: Capabilities and Related Policy Issues, Congressional Research Service Report for Congress, No. RL31787, p. 21, 19 July 2004.

150 Laurent Murawiec, "La cyberguerre", *Revue Agir*, no. 2, p. 8, December 1999.

151 Martin Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, Rand Corporation, 2009, www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.

	infrastructure is at once the target, the means and the weapon of the attack. Few actions in the real world, if any at all, accompany the attack. This type of cyberwar enables us, for instance, to slowdown the progression of the armed forces; Unrestricted cyberwar, which no longer makes any distinction between civilian and military targets; which has consequences in the physical world, particularly in terms of lethality; which may have a profound economic and social impact. Powerful nations are also very vulnerable to unrestricted cyberwar (an idea which refers to Chinese unrestricted war).[152]	Shimeall, 2001[153]
V - A subdivision of information warfare	"*Modern information and communication technology has given rise to the phenomenon of cyber warfare – information warfare carried out on the Internet*"[154]	Giles Trendle, 2002[155]
Focus on the actors		
VI - Inter-State conflict, state operation	Cyberwar is the use of computers or digital means by a government or with its explicit knowledge or approval, against another State, or private property in the territory of another State, including: intentional access, interception of data or damage caused to digital or digitally-controlled infrastructures.	United Nations Security Council, 2011[156]

152 Qiao Liang, Wang Xiangsui, *La guerre hors limites*, Paris, Rivages poche, p. 310, 2006.

153 T. Shimeall, Ph. Williams, C. Dunlevy, "Countering cyber war", *NATO Review*, CERT Analysis Center of Carnegie Mellon University & NATO, vol. 49, no. 4, pp. 16-18, 2001.

154 This definition leads us to consider as cyberwar any actions of site defacement, actions carried out by hackers whom we do not know to be military or civilians, combatants or non-combatants, immediate enemies or third parties, acting in the interest of hostiles or for fun, with a background in delinquency/criminality or the law of armed conflict. Many, many such situations have occurred over the past 20 years: during conflicts, revolts and revolutions break out, and hackers and hacktivists are active.

155 Giles Trendle, Cyberwar, "Internet warfare in the Middle East", *The World Today*, vol. 58, no. 4, pp. 7-8, 2002, http://www.chathamhouse.org/sites/default/files/public/The%20World%20Today/2002/wt020406.pdf.

156 United Nations Security Council, *Resolution 1113 (2011)*, p. 1, 5 March 2011.

	When the expression "cyberwar" is used in this book, it refers to actions performed by nation States to infiltrate the computers or computer networks of other nations, with the purpose of causing damage or disturbances.	Richard Clarke, 2010[157]
	"*Cyberwar is a conflict between States but which can also involve other non-State actors in a variety of ways. In cyberwar it is extremely difficult to have a targeted and proportionate force; the target may be military, industrial of civilian, but it may also be the site of a server hosting numerous clients, only one of which is the intended target*".	Paul Cornish, 2010[158]
	Cyberwar is "conflict *between two or more States, intended to damage the systems, processes and computer resources, and to attach the political, economic and social systems and to indoctrinate the masses to destabilize the society and the State, but also to force it to take decisions that favor the interests of an enemy party"*.	Shanghai Cooperation Organization, 2009[159]
	"*What is meant by the term 'cyberwar' is not clear. If that means an organized attack, coordinated by the government of a foreign State, the threshold is indubitably too high; it is unlikely that we shall, in the near future, see an unequivocal example, except perhaps on the part of the United States attacking its enemies' computers. The definition of the term 'cyberterrorism' is similarly unclear. However, in the same way as we distinguish between war and terrorism, this object (cyberterrorism) produces different responses than does 'cyberwar'.*"	Gary Shapman, 1998[160]

157 Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It*, Ecco, United States, p. 320, 2010.
158 Cornish Paul, Livingstone David, Clemente Dave, York Claire, On Cyber Warfare, A Chatham House Report, London, p. 49, November 2010.
159 Shanghai Cooperation Organization, Appendix I to the agreement between the governments and the Member States of the Shanghai Cooperation Organization over the question of cooperation for international security of information, 16 June 2009.
160 Gary Shapman, "National Security and the Internet", *Annual Convention of the Internet Society*, July 1998, Geneva, http://www.utexas.edu/lbj/21cp/isoc.htm.

VII - A conflict which is not limited to State actors	""Cyber war" is not a helpful term because such a conflict only exists at the far end of the spectrum of likely forms of conflict enabled by cyberspace. A 'cyber war' is an overt, more or less formally declared blend of kinetic and virtual exchanges with uniformed adversaries using cyber means to harm the other sides in the dispute. A 'cyber war' will involve large-scale organizations such as nations who declare their conflict with other states to be active in the same manner a kinetic war is declared. They openly employ all the institutional means at their disposal, including cyber tools or kinetic forces to prevail against their opponents. […] Cyberspace as a globally open, nearly free substrate, however, has generated a much wider spectrum of intergroup human conflict than 'cyber war'."	Chris Demchak, 2013[161]
VIII - A war where the individual cedes his place to the machine	Computers are the soldiers	Jonathan V. Post, 1979[162]
Focus on practices		
IX - Military operations	"Cyberwar is a set of coordinated operations carried out in cyberspace, with clearly-defined objectives, using information and communication systems. Thus, strategically-independent cyberwar is a fallacy... cyberwar does not directly include the ideas of violence, physical destruction or death, but can contribute to those phenomena".	Michel Baud, 2013[163]
	""Cyberwar would logically refer to military-inspired attempts to disrupt, deny or destroy the electronic resources of the enemy through computer-based means with the aim of attaining military victory. I would personally prefer the term 'information operations' to refer to that	Alan Chong, 2013[164]

161 Interview of Chris Demchak (US Naval War College) by Daniel Ventre, April 2013. http://www.chaire-cyber.fr/IMG/pdf/article_3_3_-_chaire_cyberdefense.pdf.
162 Jonathan V. Post, "Cybernetic wars", *Omni*, pp. 44–104, 1979.
163 Michel Baud, *Cyberguerre: en quête d'une stratégie*, Ifri, Paris, France, Focus Stratégique, no. 44, p. 47, May 2013.
164 Interview of Alan Chong (RSIS – Singapore) by Daniel Ventre, April 2013. http://www.chaire-cyber.fr/IMG/pdf/article_3_2_-_chaire_cyberdefense.pdf

	whole range of political interventions ranging from the theft of data, deception, disruption, to destruction enabled by electronic computer-based means. Information operations do not distinguish peace time from war time."	
	Cyberwar is "an armed conflict carried out either totally or partially using cyber resources – i.e. military operations conducted to prevent the enemy from making effective use of cyberspace systems and weapons during a conflict. This includes cyber attacks, cyber defense and cyber actions".	Joint terminology for cyberspace operations, 2010[165]
	Cyberspace war, combat in cyberspace[166]: components of cyber-operations (cyberOps) which extend cyber-power beyond the defensive limits of the GIG[167] to detect, dissuade and defeat adversaries. The capabilities of combat in cyberspace involve computers and telecom networks, onboard processors, controllers, systems and infrastructures.	US Army document – Training and Doctrine Command – Tradoc), 2010.[168]
	"We draw the distinction between what we call 'netwar' – society-wide ideational conflicts, carried out partly through networked communication means – and cyberwar, which is military in nature. […] a netwar which targets a C3I enemy military system becomes, at least in part, what we mean by cyberwar. […] Cyberwar refers to the conducting and preparation of military operations, in accordance with principles connected to the use of information. This means disturbing or destroying information and	John Arquilla, David Ronfeldt, 1993[169]

165 Department of Defense, Joint Terminology for Cyberspace Operations, Vice Chairman of the Joint Chiefs of Staff, United States, 2010, www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf.

166 The text begins by using the term "cyberspace warfare". Hence, thereafter, the term "CyberWar" therefore does not express "cyberwar" but instead "combat/conflict/battle in cyberspace".

167 Global Information Grid: project to create a grid showing all the capabilities and information systems of the US Department of Defense.

168 Department of Defense, *Cyberspace Operations Concept Capability Plan*, TRADOC PAM 525-7-8, 2016-2028, 22 February 2010, 80 pages: [http://www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf].

169 John Arquilla, David Ronfeldt, "Cyberwar is coming!", *Comparative Strategy*, Taylor & Francis, vol. 12, no. 2, pp. 141–165, 1993.

	communication systems, broadly defined to include military culture, upon which an adversary relies for self-knowledge: who he is, where he is, what he can do, at what time, why he is fighting, which threats to confront first, etc. – i.e. finding out everything about the enemy whilst preventing him from doing the same to us. Doing so tips the balance of information and knowledge in our favor".	
	A netwar which targets a C3I enemy military system becomes, at least in part, what we mean by cyberwar.	John Arquilla, David Ronfeldt, 1993[170]
X - Set of offensive/defensive practices	Cyberwar is a coercive action which involves computer attacks	Adam P. Liff, 2012[171]
	"Cyberwar is the systematic use of information (bits, messages) to attack information systems and, especially, the information held by that system".	Martin Libicki, 2011[172]
	Cyberspace has its own rules; for example, it is easy to mask one's identity and difficult to predict or even to understand the effects (damage) caused by a clash. Cyberwar is manipulation of ambiguity.	Martin Libicki, 2009[173]
	Cyberwar is a "*conflict that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses*"[174]	Kevin Coleman, 2008[175]

170 *Ibid.*

171 Adam P. Liff, "Cyberwar: a new 'absolute weapan'? The proliferation of cyber warfare Capabilities and interstate war", *Journal of Strategic Studies*, vol. 35, no. 3, pp. 401-428, 2012, http://indianstrategicknowledgeonline.com/web/Proliferation%20of%20Cyberwarfare%20Capabilities%20and%20Interstate%20War.pdf.

172 Martin Libicki, Cyberwar as a Confidence Game, *Strategic Studies Quarterly*, pp. 132-146, spring 2011, http://www.cyberdialogue.ca/wp-content/uploads/2011/03/Martin-Libicki-Cyberwar-as-a-Confidence-Game.pdf.

173 Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, Rand Corporation, p. 238, 2009.

174 "A conflict that uses hostile, illegal transactions or attacks on computers and networks in an effort to disrupt communications and other pieces of infrastructure as a mechanism to inflict economic harm or upset defenses".

	"Cyber warfare is symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems. It requires a high degree of interdependence between digital networks and infrastructure on the part of the defender, and technological advances on the part of the attacker. It can be understood as a future threat rather than a present one, and fits neatly into the paradigm of Information Warfare."	Shane M. Coughlan, 2003[176]
	Cyberwar can refer to various aspects of defense and attack of information and computer networks in cyberspace, and the means of preventing the adversary from doing the same thing[177].	Steven A. Hildreth, 2001[178]
XI - State operations excluding espionage	First, cyber war will be defined as consisting of computer network (more broadly, systems) attack and defense. An attack succeeds when the target's use of its own systems is hampered – either because such systems fail to work or work very efficiently (disruption) or because systems work but produce errors or artifacts (corruption). This definition specifically excludes computer network exploitation, which meets neither of these criteria. It is fair to say that CNE accounts for the great preponderance of computer network operations carried out among states and similarly serious noncriminal organizations. Yet it is a different phenomenon. Spying is not an act of war. It never has been, and there's little reason to change that.	Martin Libicki, 2011[179]

175 Kevin Coleman, *The Cyber Arms Race Has Begun*, CSO Online, 28 January 2008.
176 Shane M. Coughlan, *Is there a Common Understanding of What Constitutes Cyber Warfare?,* The University of Birmingham School of Politics and International Studies, p. 2, 30 September 2003.
177 In reality, this definition is fairly close to that of information operations. The author assimilates "information warfare", "information operations" and "cyberwar".
178 Steven A. Hildreth, Cyber warfare*,* CRS Report for Congress, Washington DC., p. 20, 19 June 2001, http://www.au.af.mil/au/awc/awcgate/crs/rl30735.pdf.
179 Martin Libicki, "Sub rosa cyber war, *in* christian czosseck", Kenneth Geers, *Cryptology and Information Security Series*, vol. 3, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Amsterdam NL (IOS Press), pp. 53-65, 2011.

A different focus		
XII - Cyberwar is not or cannot be defined: as generally accepted, it covers too many different realities	There is no common definition of exactly what constitutes a cyberwar. The attacks on Estonia in 2007, those on Georgia in 2008, the deployment of Stuxnet, today's high-level espionage… all of this has been qualified as cyberwar – even cyber attacks which have nothing to do with inter-State conflicts, such as hacktivism, or the cyber attacks that took place during the WikiLeaks scandal, or those in support of the Arab Spring revolution in February-March 2011. This would seem to imply that the concept of "warfare" is no longer strictly limited to nation States. For want of a common definition, most EU and EC Member States have avoided using the term "cyberwar" in official documents, instead preferring neutral expressions such as "cyber espionage", "cyber attacks", or "cyber defense".	European Parliament, 2012[180]
	Cyberwar exists but cannot be fully defined because of its complexity	Howard Schmidt (White House cyber tsar), 2010[181]
	Cyberwar exists but cannot be fully defined because of its complexity	General Keith Alexander, head of US Cyber Command, 2010[182]

Table 1.3. *Military and non-military definitions of cyber warfare*

180 Alessandro Giovannini, Daniel Gros, Paul Ivan, Piotr Maciej Kaczynski, Iego Valiante, External Representation of the Euro Area, European Parliament, Directorate General for International Policies, Subcommittee on Security and Defence, p. 83, 2012, http://www.europarl.europa.eu/studies.

181 From Sean Lawson, "General Alexander's confirmation and the failure of cyberwar transparency", *Forbes.com*, 13 May 2010, http://www.forbes.com/sites/firewall/2010/05/13/general-alexanders-confirmation-and-the-failure-of-cyberwar-transparency/.

182 *Ibid.*

1.4.13. *Netwar*

Netwar means network warfare. "Cyberwar" is the military version of network warfare; "netwar" is the version of network warfare in non-military society. This argument is defended by John Arquilla and David Ronfeldt (Rand Corporation)[183,184].

183 ARQUILLA J., RONFELDT D., *Networks and Netwars. The Future of Terror, Crime and Militancy*, Rand Corporation, Santa Monica, 2001.

184 An example of *netwar* was provided by the resistance of the Zapatista movement in Mexico in 1994. The movement used the Internet to mobilize public opinion, eventually managing to alter the government's decision, and to avert a planned military offensive to decimate the movement. The Net was used as a worldwide soundbox, capable of influencing the leaders' decisions. A report by Rand was devoted to that question, in 1998, entitled "The Zapatista Social Netwar". Their view is that of the emergence of a civilian form of networked warfare (cyberwar would be the military version, with that term being reserved for high-intensity conflicts). It is the use of networks by criminals, terrorists, extremists, but also by activists (cyber-activists and hacktivists). Exploiting the capabilities offered by the NICT revolution, all these actors take advantage of their networking, without necessarily needing leaders to coordinate the groups, and the possibility of communicating, acting and reacting quickly (which enables them to launch operations which States are unable to anticipate), and all without specific boundary constraints. The concept of *netwar* refers to the idea of transformation of social relations, on a worldwide scale, thanks to the development of communication networks. The concept is based on the prediction of the major role which information networks will play, from now on, in society. This social evolution is based on the technological revolution. As a case study, the authors examined the Zapatista uprising (Mexico, 1994) which, from a centralized and hierarchical movement, structured around the leaders of the insurrection movement, turned into a conflict of the Information Age – i.e. that it was characterized, according to the authors, by the mobilization of actors in the media, politicians, NGOs, beyond the national borders, whose operations of media coverage and influence exerted pressure on the Mexican government, causing it to backtrack in its repressive attitude. This *netwar*, a war of information, could be viewed as a precursor as the movements on social networks. On the basis of their observation of the Zapatista rising, the authors illustrate the characteristics of this new means of conflict: the actors must have a communication strategy; netwar modifies conflict because it tends to involve a networked form of organization rather than hierarchical models of organization, and because conflicts are increasingly dependent on information and communication; the management of perceptions is crucially important in netwar practices; psycho-social destruction is becoming more important than physical destruction; threats are becoming diffuse, dispersed, nonlinear and multidimensional; the range of actors involved in netwar is wide (criminals, terrorists, revolutionaries, activists, etc. but also pacifistic activists). Hence, there are various forms of netwars (that which we call "social netwar" refers to activism, generally non-violent in its approach); the preferred

This theory implies a new organizational structure of the opposing parties and gives an advantage to organizations that operate in the network mode (structured in units, dispersed and coordinating their common actions through networks). Arquilla and Ronfeldt define netwar as warfare in the information age:

– the parties are organizations spread as individuals and in small groups;

– the mode of contact is remote communication to coordinate activities and conduct operations. Parties are therefore interconnected;

– the structure is distributed; there is no hierarchy and no centralization.

This type of warfare through networks adapts to amorphous groupings such as terrorist organizations, and it is the type of warfare that, for example, "hacktivists" carry out, activists or international hacker groups acting as one group but often made up of individuals spread over several geographical territories.

Authors	Concepts
John Arquilla, David Ronfeldt	Netwar (2001), Cyberwar (1993)
Cebrowski, Rumsfeld	Network centric warfare – NCW (1998)
John Boyd	OODA loop

Table 1.4. *Authors and concepts*

method must be swarming (which consists of concentrating all forces on one or various points simultaneously); information technologies may represent a threat of destabilization for governments; favorable conditions must be created to facilitate netwar (a significant worldwide civil society; non-authoritarian regimes; local NGOs capable of forming alliances with national and transnational NGOs; a government which attaches a great deal of importance to its image on the international scene; mobilization of a wide audience outside of the immediate conflict zone), so not all societies are capable of staging netwars.

2

China

2.1. Significant publications

A great deal has been written on China's policies, strategies and doctrines, as regards information warfare (essentially from 2000 onwards), over the course of the past two decades. Over the past ten years, there has been a specific focus on cyberwar (or cyber warfare).

In regard to China and its role in the NICT sector, discourse tends to oscillate between two approaches:

– one focuses on China's economic potential, the pace of its technological development, and the promise of its enormous national market;

– the other, though, is concerned with these industrial and technological developments, China's increasing power on the world market, the potential threat to national security which could be posed by the use of Chinese products in certain key infrastructures or sectors (certain national markets have been closed to Chinese products). Subscribers to this approach also worry about the developments of the Chinese army – particularly (though not exclusively) in cyberspace; the aggressive desires of the agencies in charge of cyberespionage;

Information Warfare, First Edition. Daniel Ventre.
© ISTE Ltd 2016. Published by ISTE Ltd and John Wiley & Sons, Inc.

and indeed China's positions in international bodies pertaining to the worldwide governance of the Internet. The negative approach also offers a criticism of Chinese policies which restrict freedom of expression on networks. The topic of the "Chinese cyberthreat" is a component of the "Chinese threat" which is found in a number of other domains: the economy, the army, politics, ecology, etc.

There have been numerous publications (reports, articles and books) on Chinese information warfare (and information operations) over the course of the past 15 years. Let us recap the most significant of these: Ahari, M. Ehsan, 1997[1]; E.N. Dezhin, 1999[2]; K.L. Gauthier, 1999[3]; James Mulvenon, 1999[4]; Toshi Yoshihara, 2001[5]; Kate Farris, 2001[6]; Vincent Wei-cheng Wang, 2002[7]; Robin E. Ferguson, 2002[8]; Edward Sobiesk, 2003[9]; Vincent Wei-cheng Wang, 2003[10]; Timothy

1 M. Ehsan Ahari, "Chinese prove to be attentive students of information warfare", *Jane's Intelligence Review*, vol. 9, no. 10, pp. 469–473, October 1997.

2 E.N. Dezhin, "Information warfare as chinese analysts see it", *Military Thought*, vol. 9, no. 6, pp. 82–85, 1999.

3 K.L. Gauthier, "China as peer competitor", *Trends in Nuclear Weapons, Space, and Information Warfare*, Technical Report, Air War College, USA, 1999.

4 James Mulvenon, "The PLA and Information Warfare", in James C.M., Richard H.Y., *The People's Liberation Army in the Information Age*, RAND Corporation, USA, 1999.

5 Toshi Yoshihara, Chinese Information Warfare: A Phantom Menace or Emerging Threat?, available at: http://www.au.af.mil/au/awc/awcgate/ssi/chininfo.pdf, 2001.

6 Kate Farris, "Chinese views on information warfare", *Defence Intelligence Journal*, vol. 10, no. 1, pp. 37–58, Winter 2001.

7 Vincent Wei-cheng Wang, "Asymmetric War? Implications for china's information warfare strategies", American Asian Review, vol. 20, no. 4, p. 167, December 2002.

8 Robin E. Ferguson, Information Warfare with Chinese Characteristics: China's future view of information warfare and strategic culture, available at: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA416897, 2002.

9 Edward Sobiesk, Redefining the Role of Information Warfare in Chinese Strategy, SANS Institute, available at: http://www.sans.org/reading-room/whitepapers/warfare/redefining-role-information-warfare-chinese-strategy-896, 2003.

10 Vincent Wei-cheng Wang, "China's information warfare discourse: implications for asymmetric conflict in the taiwan strait, issues & studies", vol. 39, no. 2, pp. 107–143, 2003.

L. Thomas, 2003[11], 2004[12], 2007[13]; Paul J. Bolt and Carl N. Brenner, 2004[14]; Barrington M. Barrett, 2005[15]; Gary D. Rawnsley, 2004[16]; Vinod Anand, 2006[17]; William G. Perry, 2007[18]; A.A. Migunov, 2008[19]; Daniel Ventre, 2011[20]; Monika Chansoria, 2012[21]; William Hagestad, 2013[22]; I. Vasiliyeva, Y. Vasiliyeva, 2013[23]; V. Inna,

11 Timothy L. Thomas, Like Adding Wings to a Tiger – Chinese Information War Theory and Practice, *Military Intelligence Professional Bulletin*, vol. 29, no. 3, pp. 22–27, July-September 2003.

12 Timothy L. Thomas, Russian and Chinese Information Warfare: Theory and Practice, FMSO, June 2004, 56 pages, USA, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467510, 2004.

Dragon Bytes: Chinese Information-War Theory and Practice From 1995-2003. Fort Leavenworth, KS: Foreign Military Studies Office, p. 16, 2004.

Timothy L. Thomas, Comparing US, Russian, and Chinese Information Operations Concepts, available at: http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf, 2004.

13 Timothy L. Thomas, Decoding The Virtual Dragon – Critical Evolutions In The Science And Philosophy Of China's Information Operations And Military Strategy – The Art Of War And IW, Foreign Military Studies Office (FMSO), Washington, 2007.

14 Paul J. Bolt & Carl N. Brenner, "Information warfare across the Taiwan strait", *Journal of Contemporary China*, vol. 13, no. 38, 2004.

15 Barrington M. Barrett, "Information Warfare: China's Response to U.S. Technological Advances", *International Journal of Intelligence and Counter Intelligence*, vol. 18, no. 4, 2005.

16 Gary D. Rawnsley, "Old wine in new bottles: China-Taiwan computer-based 'information warfare' and propaganda", *International Affairs*, vol. 81, no. 5, pp. 1061-1078, 2004.

17 Vinod Anand, "Chinese Concepts and Capabilities of Information Warfare", *Strategic Affairs*, vol. 30, no. 4, October 2006.

18 William G. Perry, "Information Warfare: An Emerging and Preferred Tool of the People's Republic of China", *The Center for Security Policy, Occasional Papers Series*, no. 28, p. 11, Washington DC., October 2007.

19 A.A. Migunov, "Trends of China's Strategy in Information Warfare", *Military Thought*, vol. 17, no. 4, pp. 142–148, 2008.

20 Daniel Ventre, "Riots in Xinjiang and Chinese information warfare", in Daniel Ventre (ed.) *Cyberwar and Information Warfare*, ISTE-Wiley, 2011.

21 Monika Chansoria, "Defying borders in future conflict in East Asia: Chinese capabilities in the realm of information warfare and cyberspace", *Journal of East Asian Affairs*; vol. 26, no. 1, pp. 105–127, Spring/Summer 2012.

22 William Hagestad, *Chinese Information Warfare Doctrine Development 1994 – 2014*, Red Dragon Rising Publishing, November 2013.

William Hagestad, *China's Plans for Winning Information Confrontation: Important Chinese Information Warfare Articles*, Red Dragon Rising Publishing, 2014.

2013[24]; Larry Wortzel, 2014[25]; Brig Vinod Anand, 2014[26]; Dean Cheng, 2014[27]; Taylor Fravel, 2015[28].

These publications on Chinese information warfare essentially concentrate on the following points:

– the revolution in military affairs (RMA) in the Chinese forces (PLA – People's Liberation Army);

– the actors in contemporary strategic thinking, and the ancestral roots of that school of thought (Sun Tzu);

– the key concepts feeding into strategic thinking and doctrine;

– the peculiarities of Chinese thinking and the traits which set it apart from the rest of the world (is Chinese thinking "different"?)

– China's various practices, or those attributed to it, pertaining to information warfare;

– the actors involved in information warfare, and the organization in the forces;

23 I. Vasiliyeva, Y. Vasiliyeva, "Thirst for Information: The Growing Pace of Information Warfare and Strengthening Positions of Russia, the USA and China", *Proceedings of the 8th International Conference on Information Warfare and Security (ICIW-2013)*, Academic Publishing International Limited, UK, 2013.

24 V. Inna, "The Value of Interaction for Russia, the USA and China Facing the Information Warfare", *International Journal of Cyber Warfare and Terrorism*, vol. 3, no. 4, pp. 1-9, 2013.

25 Larry Wortzel, *The Chinese People's Liberation Army and Information Warfare*, Create Space Independent Publishing Platform, March 2014.

26 Brig Vinod Anand, PLA's Information Warfare Capabilities on an upward trajectory, available at: http://www.vifindia.org/article/2014/april/21/pla-s-information-warfare-capabilities-on-an-upward-trajectory, 2014.

27 Dean Cheng, "PLA views on Informationized Warfare, Information Warfare and Information Operations", in Daniel Ventre (ed.), *Chinese Cybersecurity and Defense*, Wiley, 2014.

28 Taylor Fravel, "China's New Military Strategy: Winning Informationized Local Wars", *China Brief*, vol. 15, no. 13, June 2015.

– the place occupied by information warfare in China's international relations: tensions with Taiwan, with Japan, with the United States, etc.;

– the perception of Chinese information warfare in the world (a strategy and constitutive practices of the Chinese "threat").

The work on cyber security, cyber defense or cyber attacks focuses essentially on international analyses of the past 10 years, on Chinese defense strategy based on the use of NICT, cyberspace and information. These works win out, in terms of volume, over approaches which focus more specifically on information warfare, on information operations, and on the security issues relating to the use of the informational domain.

China, for its part, discusses its defense strategies and doctrines on a number of channels: White Papers, "The Science of Military Strategy", articles in military and academic journals, press-agency articles[29] or army Websites, official declarations books (seminal works, such as the monograph by Shen Weiguang published in 1986[30], and sometimes publications with worldwide success such as Unrestricted Warfare)[31], and Chinese translations of foreign books on the subject.[32]

Since the 1990s, China has been analyzing the concept of information warfare with great interest. Military strategists have

29 A few examples:
- "China's military forces to be trained for informationized warfare", 5 March 2009, *People's Daily Online*, http://en.people.cn/90001/90776/90785/6606504.html.
- "Armies to be trained for informationized warfare", available at: http://china.org.cn/government/NPC_CPPCC_2009/2009-03/05/content_17377590.htm.

30 Shen Weiguang, *Information Warfare*, Zhejiang University Press, China, March 1990.

31 L. Qiao, X. Wang, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, China, February 1999.

32 The first edition of this book, Information Warfare, 2009, was also translated into Chinese and published in Beijing in 2013.

formulated a new warfare doctrine and theories on information warfare. Marked by their cultural characteristics, these theories are compliant with Chinese thinking, and aspire to offer solutions to reach medium- and long-term political objectives set by the government, and face the immediate threats perceived by the country.

2.2. Strategic and doctrinal thinking about information warfare. Genesis

The resounding success of the American military during the First Gulf War, the famous "Desert Storm" campaign, quickly showed the obvious superiority that information control gives the military. The concept of "information warfare" became obvious to China in this context, and China then committed itself to a profound theoretical reflection, involving significant ideological studies resulting in abundant literature on the subject. Reading through the work of the most important and most frequently quoted authors, we can trace the genesis of the "information warfare" concept in the Chinese world.

The English translations of Chinese articles, published in 1997 by the National Defense University Press in a book entitled *Chinese Views of Future Warfare* laid down the first useful foundations for understanding that Chinese school of thought. The articles by Wang Pufeng[33], Wang Boacun and Li Fei[34] and Wei Jincheng[35] are specifically devoted to information warfare. That book, firstly because of the breadth of the spectrum of defense issues which it discusses,

33 Wang Pufeng, "The Challenge of Information Warfare", in Michael Pillsbury (ed.), *Chinese Views of Future Warfare*, National Defense University Press, Washington, DC, 1997.
34 Wang Boacun, Li Fei, "Information Warfare", in Michael Pillsbury, (ed.), *Chinese Views of Future Warfare*, Washington, DC, National Defense University Press, 1997.
35 Wei Jincheng, "Information War: A New Form of People's War", in Michael Pillsbury (ed.), *Chinese Views of Future Warfare*, National Defense University Press, Washington, DC, 1997.

and secondly because of the scarcity of translations in English making Chinese writings accessible, is one of the founding elements of Western analysis of China's defense strategies and doctrines.

Chinese Views of Future Warfare is a collection of contributions from Chinese authors covering a broad spectrum of defense issues. All these works are guided by and refer to the strategic thinking of Deng Xiaoping. Thus, the first part of the book is entitled *The Strategic Thought of Deng Xiaoping*: it speaks about the modernization of defense, of war and peace, of active defense and of popular warfare. The second part is intended to be more prospective: "Future Security Trends", focusing specifically on the challenges in the Asia-Pacific zone and on future security crises. The third part specifically discusses the process of modernization of forces with a view to preparing for local wars: modernization of logistics, nuclear weapons, armaments, industrial reform, the science and technology of defense, and dialectic issues. Finally, the fourth part, entitled "The Revolution in Military Affairs", speaks about 21st-Century weapons, naval warfare, aerial and terrestrial warfare, modern operations, conceptual developments, tactical studies, and nano-technological weapons. It is in this final part that the three articles on information warfare appear.

2.2.1. *General Wang Pufeng: one of the pioneers*

In 1995, General Wang Pufeng emerged as the father of the Chinese information warfare doctrine. He was impressed by the superiority of the Americans, acquired in part by satellite reconnaissance systems during the Gulf War, which made it possible to locate strategic sites, enemy positions and attack Iraqi C2 systems with precision.

His article "The challenge of information warfare", translated and published in 1997 in the United States, begins with references to American military thinking: "Andrew Marshall of the Pentagon believes the information era will touch off a revolution in military affairs […] U.S. Army Chief of Staff General Gordon Sullivan holds

that the information era is changing the army […] U.S. Secretary of the Army Togo West says […] The U.S. Army believes that […] The U.S. Army has presented the concept of Force 21 […] The U.S. Army has taken these actions to prepare for future information warfare"[36]. The author, if not the Army itself, has the same convictions as the Americans: information (and with it, computerization, digitization of the battle arena and networking of the forces) is a majorly-important factor, which conditions military power, and hence the ability to win wars.

The article continues with an observation: the Chinese Army is – in terms of its constitution, its organization, its armament – the product of the industrial era. Thus, modernization is required, because in the mid-1990s, the Chinese Army was not suited to information warfare. However, this adaptation is of crucial importance, because firepower and military superiority depend directly on informational superiority, points out General Wang Pufeng. This adaptation is not only necessary but vital, because information will be at the heart of conflicts to come with powerful enemies. This adaptation must also aim to win wars, leading to the defeat of more powerful enemies, at a lesser cost.

The adaptation of forces for information warfare requires the development of new capabilities, the training of the military and the formalization of a theory of information warfare.

Indeed, in the information age, he goes on, it is no longer so much the military capabilities (number of soldiers, weapons, power of armaments) which count, as the capacity to use these resources – a capacity which is determined by information. The modernization of the Chinese Army thus no longer needs to aim to reproduce the principles of the industrial era, but instead to develop around capabilities specific to information warfare (information technologies, information weapons systems, networking). Military personnel need

36 Wang P., *Meeting the Challenge of Information Warfare*, Zhongguo Junshi Kexue, Beijing, February 1995.

to be trained in this new form of warfare. This modernization also needs to be underpinned by the theory of information warfare, which draws on the Marxist and Maoist strategy of war, and makes an effort to think about the use of information to defeat enemies with superior military capabilities. This asymmetry differs, though, from that which had been in place up until then, the author estimates, because the combat essentially takes place in an intangible space – a computer battlefield.

The modernization of the forces takes place on various levels. The first of these is material: computerized weapons systems, network infrastructure, information weapons such as precision-guided weapons, electronic warfare weapons and C4I systems. These "information weapons" do not include malware, and are not equivalent to what is called "cyber weapons" hereinafter. At this point, we are still on the hardware layer. Information weapons refer more to weapons which are computerized, systems which constitute the nerve center of the whole defense architecture, aerial defense systems and tactical missile systems. The construction of a defense network, including a digitized battlefield, must aim to facilitate the sharing of information ("information may be shared on the network"). Yet just as important as sharing is control of the information.

Information warfare must be one of the key capabilities of Chinese active defense strategy. General Wang Pufeng distinguishes two forms of information warfare: one defensive; the other offensive. He uses the example of America's surprise attack on Libya and the experience of the Gulf War to identify the various components of these two aspects of information warfare. As is shown in Table 2.1, based on Wang Pufeng's text, a fair number of these elements making up the offensive and defensive aspects of information warfare include components that pertain more to electronic warfare and kinetic actions (e.g. bombing buildings that host communication systems).

Offensive information	
	Information reconnaissance to gain information on targets
	Electronic interference (for instance, "using counter radiation guided missiles to destroy air defense radar stations")
	Information suppression
	Information attack by using precision-guided warheads
	Computer viruses were used to destroy the computer systems
	Launch precision-guided bombs against the communications building
Defensive information	
	Counter reconnaissance: "secret falsification can be used to plant false intelligence and false targets"
	Resistance to interference
	Resist viruses
	Information counterattack

Table 2.1. *Offensive and defensive components of information warfare. From Wang Pufeng, 2007*

In a conflict, the confrontations will use one or other of the two forms of warfare (offensive and defensive). Also, information actions are not exclusive: they take place in support of, in addition to, in furtherance of the offensive and defensive actions here referred to as "strategic". The information actions are not limited to the duration of the war. However, outside of armed conflict, information weapons are not used.

2.2.2. *Wang Baocun and Li Fei*

The article by Wang Baocun and Li Fei is simply entitled "Information warfare"[37].

37 Wang Boacun, Li Fei, "Information Warfare", in Michael Pillsbury, (ed.), *Chinese Views of Future Warfare*, Washington, DC, National Defense University Press, 1997.

Once again, the authors begin their article which a reference to American military statements: "In *Army* magazine (1994), Lieutenant General Cerjan, former U.S. National Defense University President, notes, 'Information warfare is a means of armed struggle' […] General Sullivan, U.S. Army Chief of Staff, holds that 'information is the most crucial combat effectiveness', […] A U.S. combat theory analyst sums up the substance of information warfare in six points". These are all explicit references which demonstrate the extent to which American thinking and practices help to shape China's thinking in this area. The reflections given are inspired by observation of American experience: "While information warfare in the true sense has not yet arrived in the battlefield arena, the repeated live-troop maneuvers and simulated drills of the armies of Western nations such as the United States, as well as the Gulf War, have enabled us to determine certain innate features of information warfare"[38]. The authors also cite Alvin Toffler[39].

The article is careful to define the concept of information warfare. Wang and Li first offer an overview of the definitions commonly formulated by Chinese experts. In their collective view, the essence of information warfare lies:

– in combat operations which take place in a high-tech battlefield;

– where the combatants employ resources, equipment and systems based on information technology (i.e. computer systems);

– where the objective is the acquisition of information superiority (the power to obtain, control and use information) and the have the initiative;

– where the clashing forces are computerized (i.e. connected) units;

– where all sorts of information weapons (smart weapons) are used;

– where the operations are offensive and defensive (deception and antideception; destruction and antidestruction of information, etc.).

38 Page 330.
39 Page 339.

Table 2.2 gives an overview of the components of information warfare as identified by the various authors:

Components of information warfare	Deception
	Operational secrecy
	PSYOPS
	Electronic warfare
	Substantive destruction of information systems (including personnel)
	Computer virus warfare
Objectives	To disrupt the enemy's information flow
	"Destroy the enemy's command and control capability"
	"Keeping one's own command and control capability from being affected by similar enemy actions"
2 general areas	Information protection (defense)
	Information attack (offense)
Key targets	"The enemy's combat command, control and coordination, intelligence, and global information systems"
3 prerequisites	"The capability to understand the enemy's information systems, and the establishment of a corresponding database system"
	"Diverse and effective means of attack"
	"The capability to make battle damage assessments [BDA] of attacked targets"
Characteristics	Battlefield transparency
	Overall coordination

	Operations in real time
	Precision strike
Impact on combat concepts	The struggle for information dominance will be particularly intense
	The loss of information dominance may paralyze an army and its capacity to act
	It will become increasingly difficult to win a war (no more will it be sufficient to simply exterminate the enemy or destroy their arms industry. We must now also destroy their information systems).
	Information warfare pushes the limits of warfare into space, because it is there that the central systems of information warfare are based. Let us point out here that few later publications have focused on this spatial dimension of information warfare.
	The length of the battle will be shorter: precision strikes, more precisely defined targets, focused attacks on C2. Add to this the fact that wars are no longer waged to subjugate or totally destroy one's enemies, but instead to serve limited political objectives. On this point, the authors do not back up the relation that they establish here between the motives behind the political objectives of war and information warfare. Where does the relationship between the two come from, and what is that relationship exactly?
	The combats will be more integrated: all the systems being computerized, connected, streams of information will irrigate the land army, navy and air forces and facilitate their integration

Table 2.2. *Characteristics of information warfare. Reconstructed from Wang Baocun and Li Fei, 1997*[40]

40 Wang Boacun, Li Fei, "Information Warfare", in Michael Pillsbury, (ed.), *Chinese Views of Future Warfare*, Washington, DC, National Defense University Press, 1997.

2.2.3. *Wei Jincheng*

The article by Wei Jincheng[41] establishes the relation between information warfare and popular warfare.

The author states a number of the fundamental principles of information warfare:

– networks, information highways and computers cannot only be useful for trade or communications, but also for fighting. Networking transforms each system into a potential target. To become a combatant, an aggressor on the information networks, we merely need to understand and to know computers. Thus, not all of the actors involved in information warfare are military;

– information weapons should not be understood as only denoting computerized systems, such as precision-guided weapons. Information itself is a weapon. It can be used to attack enemy systems proactively or reactively, either immediately or after an incubation period;

– it is the role and responsibility of everyone to protect information. It is not only military information which is sensitive, and needs to be protected with secrecy;

– intelligence is not only the role of the intelligence agencies;

– information warfare, which is low-cost, exhibits relatively little risk, because the "enemy country can receive a paralyzing blow through the Internet, and the party on the receiving end will not be able to tell whether it is a child's prank or an attack from its enemy"[42];

– in the context of information warfare, popular warfare is waged by millions of individuals. Their mobilization is based on the effectiveness of information technologies. This effectiveness means that, through the networks, individuals can be mobilized politically,

41 Wei Jincheng, "Information War: A New Form of People's War", in Michael Pillsbury (ed.), *Chinese Views of Future Warfare*, Washington, DC, National Defense University Press, 1997.
42 Page 411.

"sending patriotic e-mail messages, and setting up databases for traditional education"[43].

2.2.4. *Colonels Qiao Liang and Wang Xiangsui: unrestricted warfare*

Other publications have fed into China's debates about information warfare. The work of Colonels Qiao Liang and Wang Xiangsui has gained widespread international success.

In the middle of the 1980s, China started to develop a new generation of combat forces. But in 1991, with the Gulf War, Chinese Army strategists recognized the gap between Chinese and American potential.

The Iraqi Army, equipped with Soviet and Chinese weaponry, in many ways similar to the Chinese Army at the time, was defeated in 42 days, collapsing under American fire power, the speed of intervention and the efficiency and superiority of high-tech equipment. Any Chinese victory seemed highly improbable during a possible armed conflict against the United States. Quick modernization of the Army and defense systems was in order. The Gulf War also raised awareness of the necessity to obtain control of information, and information and communication systems, in order to act more quickly and efficiently than the opponent. Reflections on the reform of the Chinese Army had to be totally reorganized in light of Gulf War lessons: the performance of the American military in the Desert Storm campaign confirmed the greater power of the United States. One of the keys to this quick victory was the control of information warfare. For some, the Gulf War became a model for future wars, but for others it was no more than a field of experimentation expecting very different wars in the future with the Desert Storm campaign as a foundation. The common point in all approaches was the obviously crucial role now played by new technologies. The way was opened up for a multitude of articles, conferences and reports on the theme of the introduction of information technologies in armies, on the role of information and

43 Page 411.

information technologies in the course of war, on what the army should be in the information age, and on information warfare.

During the following years, other wars served as examples and were used to feed reflections: the Kosovo conflict (Allied Forces operations, 1999), once more fought by opposing countries with very unequal power, supplied material for Chinese strategists, confirming conclusions from the Gulf War. In this conflict, the Serbian resistance impressed the Chinese. The concept of asymmetric war, where victory over a technologically-superior enemy was possible, became obvious.

China then became particularly interested in the concept of information warfare, its role in the strategy and development of asymmetric war solutions.

This is the context in which colonels Qiao Liang and Wang Xiangsui published a book in 1999 that has become a standard reference: *Unrestricted Warfare*[44]. The book is made up of their reflections on strategy, and reveals in part, contemporary Chinese thinking. It is also a reflection on the dominant military power of this century, the United States. And finally, it is a reflection on China's place in a world that was deeply troubled during the last decade of the last century. The text has two parts: the first involves "the new form of war"; the second discusses "the new art of war". Summarizing the book in a few lines, or even a few pages, is not an easy task as it is so rich in ideas and original points of view for Western readers; here, however, we retain only the major themes.

2.2.4.1. *A series of observations on the modern world*

Major changes occurred in the world during the last decade of the 20th Century which seem to have oriented our civilization in a different direction.

There were political and military disruptions: the Gulf War changed the face of the world, followed by several wars in Kosovo

44 Qiao L., Wang X., *Unrestricted Warfare*. PLA Literature and Arts Publishing House, Beijing, China, February 1999, 228 pages. Full text available at http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf .

and Bosnia. The fall of the Soviet Union modified the balance. There were social, technological and economic upheavals: the Internet massively entered modern societies to revolutionize them; new risks emerged; and monopolistic companies started to dominate the global economy; finally, there was the Asian financial crisis. World balances changed, revolutionized. Consequently, we must adapt the way in which we view the world and the way we fight wars.

2.2.4.2. *Governments no longer battle each other the same way*

For all its importance past and present, the Gulf War must not become a myth: "this war was not a masterpiece of military art, but […] a luxurious salon of high-tech weapons".

Qiao Liang and Wang Xiangsui suggest that it is vital to take a step back from the victory and the demonstration of American power. The United States won because of the wide imbalance between the forces. If this war was important, even though the victory was followed by a series of failures, it is mostly because it profoundly changed the way to fight a war. The military is no longer alone on the scene anymore; conflicts have become more complex. We no longer fight wars as before, using only armed methods:

> "War will have to be revived in another form and in another arena […] the financial attack […], the terrorist attack […], the attempt […], chaos […], over the Internet […] represent a half war, an almost war, a sub-war, in short the embryonic form of a new type of war".

Destruction is probably no longer the most appropriate solution to win a war: "technical progress […] offers many new possibilities of conquering. And this all makes us think that the best way to be victorious is to control and not to kill".

The authors qualify these new weapons as "soft" weapons satisfying a new war ethic (preserving human lives), "computer weapons are the most obvious example of soft weapons". Man wants to move away from the reality of trench wars, battlefields, hand-to-hand combat, slaughter, the slaughterhouse, wars where man is only cannon fodder, general killings, with its announced grand finale, the

nuclear war liable to erase humanity from the Earth: “what is the purpose of conquering an enemy if that means risking destroying the world?”.

In this new global order, governments no longer only fight through armed conflicts to reconfigure balances. There is a whole range of hostile acts: attacks in the economic, religious, financial, political, ecological and technological fields.

Traditional war as we know it no longer exists. If war has changed, it is because it has experienced “the transformation of modern technology and the market system”. Wars are now made up of different forms of non warlike actions taken alone, giving new conflicts a profile that they could not have before. This form of modern war, which the authors call “out of bounds war”, means that there are many weapons and techniques, that the “battlefield will be everywhere” and that there will no longer be boundaries between war and peace. The way to fight a war changes because the soldier moves away from the traditional battlefield, from fire and blood. At least that is what he or she is trying to do: fighting a war from afar. It changes because civilian society interferes in military affairs. As proof, remember the hacker trying to get into military information systems. A financier or a speculator can attack a country by means other than traditional weapons. Non-military personnel can carry out hostile actions against governments. The non-military war is carried out by religious, ideological or political organizations that do not respect any law, for an unlimited war with unlimited means: “the major warmongers are no longer only sovereign States […]. Sects […], the mafia […], terrorist organizations […], drug cartels […], hackers […] can become military or non-military warmongers” and their attacks “can be considered war actions intended to force another state to satisfy its own interests and requirements”. The army is no longer the only guarantor of national security; “the military pillar alone is far from being able to support the security vault of the modern national building”. “The battlefield is now here and the enemy is online”, “it is permanent war”. Modern war tactics are adding and combining different types of war tactics: military tactics (nuclear, traditional, biochemical, ecological, spatial, electronic and terrorist wars), supra military (diplomatic, network, intelligence, psychological,

technological, contraband, drug or even virtual wars), and non-military (financial, commercial, regulatory, media, ideological wars and war for resources). The Gulf War of 1991 was a traditional, diplomatic, sanction, psychological and intelligence war. The dominant weapons used in these new wars are no longer single weapons but an "integration of systems", and they are part of larger systems. The out of bounds war consists of finding the solution to a problem in a wider field than the problem itself.

2.2.4.3. *Reflection on the importance of technique*

Modern society is dominated by technique. But there are so many new techniques in the world in which we live in that none can pretend to give its name to the era, as we could, for example, with the age of electrification, or the age of steam. No technique dominates. To speak of the "Information Age" is not satisfying, because there are also nuclear technologies, biotechnologies and nanotechnologies. Which technology can dominate or include all the others? There does not seem to be any. But we can obviously not deny the importance of information technology that has a stimulating, binding and integrating power. That is how it is revolutionary.

The common characteristic of modern technologies is integration. The permanent novelty does not really come from the invention of new techniques as much as from the association, combination and integration of existing techniques amongst each other. Integration is the key to social progress, at least as much as the invention of new techniques. "These desires to use the magic of high-technology to work some alchemy on traditional weapons so that they are completely remade have ultimately fallen into the high-tech trap involving the endless waste of limited funds and an arms race."[45] We are in the age of integration of techniques, of extremely expensive techniques. "Based on weight, the B-2, which [costs] $13– $15 billion each, is some three times more expensive than its equivalent weight in gold."[46]

45 *Unrestricted Warfare*, page 23.
46 *Unrestricted Warfare*, page 24.

"Technology is the Totem of Modern Man", and novelty has become a cult. The obsession for new technology and general fusion of techniques is the main characteristic of our era and of course the field of war, like others, is affected by this phenomenon.

If we believe the reflections of the two authors on the relative importance of technologies taken separately, and the added value of integration, information technology alone cannot guide the revolution in military affairs. Integration can also go beyond the integration of techniques to expand to the integration of the military, its doctrine, commands and strategies. The key to success, to novelty and difference resides in the way we combine techniques, structures and organizations.

2.2.4.4. *Dependence on technique*

Speaking of "American devils", who "are not necessarily the only leaders in everything", Qiao Liang and Wang Xiangsui think that "they are slaves to technology in their thinking". Which would imply that the Chinese are not?

Again according to the two authors, Americans are not able to develop a thinking on a new concept of weaponry, but only on new design weaponry (i.e. new weapons). By "new concept of weaponry", we mean being able to consider as a weapon all the different ways that exceed the military field. Anything that can benefit the world can harm it. Everything can become a weapon: "a single market crash… a single invasion by a computer virus, a simple rumor... all these actions can be put in the category of new weapon design". "The new design of weaponry results in weapons closely linked to the life of civilian populations".

2.2.4.5. *On information warfare*

War feeds new techniques and new techniques feed war. But today "a war can no longer be represented by the name of the weapons used", because no single weapon can launch a revolution in military affairs.

In the past, a weapons revolution led to a revolution in military affairs. The appearance of brass, iron, the arrow or aircraft in turn considerably modified the military. Today, wars are fought with weapons systems; therefore no weapon can represent a war. We use wide technical concepts to replace them. We now speak of "information warfare" and "high-tech war".

Information warfare is not the same as computer warfare. Information warfare is the "war where information technology is used to obtain or destroy information". Computer warfare combines all forms of warfare "enhanced and accompanied by information technology".

"The Out of Bounds War – the Art of the Asymmetric War between Terrorism and Globalization" actually says very little about information warfare, reducing it to intelligence warfare. But these few words contain so many actions: collecting information with ISR systems; giving a central place to intelligence, espionage by networks; using open-source knowledge available over the Internet; and intercepting communications. "Destroying information" is an action that is just as wide and can include the destruction of information by network attacks, the destruction of ISR methods and the interruption of observation satellites, mixing physical and logical attacks.

2.2.5. *General Dai Qingmin and Wang Baocun*

In the April 2000 publication of the *China Military Science* magazine, making its mark for its series of articles on information warfare, General Dai Qingmin[47], who was the commander of the information warfare center in Wuhan, attempted to define information by moving away from the American model.

He is a supporter of preemptive attacks, in taking the initiative and achieving superiority of information. In this attitude, he is in contradiction with the official strictly defensive strategy (active

47 Dai Q., *Innovating and Developing Views of Information Operations*, Zhongguo Junshi Kexue, Beijing, April 2000.

defense) of the Chinese Army, which officially confirms the purely defensive character of its politics and does not define itself as a militarily attacking country. It does not declare war or aggressions but engages in a war only to defend national sovereignty and territorial integrity. It only attacks after having been attacked. Cyberspace, military or civilian violation is, for China, as important as a violation of national sovereignty. It does not take initiative, it reacts. This active defense doctrine is widened today to the concept of legitimate defense and preemptive attack, in reaction to a threat to national sovereignty. China has, however, often been the initiator (from our Western point of view?) and strives to define all wars conducted by the army as strictly "defensive" wars. In matters of defense, General Dai Qingmin suggested the Serbian model (Kosovo war), an active defense model (positive defense) that made it possible to defeat the Americans, but not the Iraqi one which he considers as passive (a negative defense). The Serbian defense consisted of implementing different measures such as concealment of planes and armored vehicles, the dispersion of troops in the population, methods to avoid reconnaissance tools, decoys to attract missiles, use of the Internet to broadcast information on NATO attacks and DoS type attempted attacks against NATO sites.

His article, "Innovating and developing views of information operations", defines information operations as a series of operations carried out in an information environment in place of a battlefield, using military knowledge, and using information as a direct operational target and using electronic warfare and computer network warfare as the main form. The strategy can be different based on the technological conditions influencing it. In information operations, traditional strategies can find their place and new ones emerge. But the most important thing is the capacity of the strategy to compensate for technological gaps. China is convinced that strategy can conquer technologically-superior enemies. It is used to asymmetric wars, having fought and won by strategy, over past centuries, against enemies who were militarily and technologically superior to it (fighting against Japanese invaders, and against the Kuomintang), according to Dai (see footnote 47). In the context of information warfare, in terms of strategy, we mean, for example, sabotage of enemy information

systems, weakening of the enemy's informational strike capabilities, dispersion of enemy forces, propagation of false information and launching surprise attacks against information systems. The strategy proposed by Dai Qingmin in *Innovating and Developing Views of Information Operations* is based on electronic warfare, physical destruction, computer network attacks (jamming, sabotage of enemy information systems and weakening of the enemy's capabilities to launch information warfare), dispersion of enemy forces by concentrating our own forces, diverting enemy reconnaissance efforts, giving a false impression to the enemy and launching a surprise information attack, blinding and deafening an enemy with false information, disrupting enemy reasoning, making an enemy believe that what is true is false and vice versa, leading an enemy to make a false assumption and carry out the wrong action. Superiority of information must be reached by any means and information operations must be considered from an active offensive point of view.

Another major point in its development is the importance given to integration. Not integration in strictly military operations so much as integration of military and civilian forces, the participation of civilians in the war effort, using the ideas of "people's war" expressed a few years earlier by Wang Pufeng (1995).

In the same April 2000 publication of the *China Military Science* review, Wang Baocun[48] published an article titled "The current revolution in military affairs and its impact on the Asia-Pacific region". Information warfare is presented as a form of combat action attacking the information and information systems of the enemy, while protecting one's own information and information systems. The content of information warfare is military security, military deception, physical attack, electronic warfare, psychological warfare and netwar. The vital goal of information warfare is to acquire dominance of information and retain it. This definition is greatly influenced by the American model.

48 Wang B., *The Current Revolution in Military Affairs and its Impact on Asia–Pacific*, Zhongguo Junshi Kexue, Beijing, April 2000.

2.2.6. *General Niu Li, Colonel Li Jiangzhou and Major Xu Dehui*

A third article, and just as important, was published in the April 2000 military review by Niu Li, Li Jiangzhou and Xu Dehui[49]. The authors address information warfare in the sense of "methods and processes designed and used for commanders and commanding forces to seize information supremacy on the basis of clever methods, making it possible to win information warfare at a relatively low cost".

The originality of the definition consists in approaching information warfare with the help of terminologies ("methods", "processes") from industry instead of from the military environment. In addition, guarantee of success is not only due to superiority of information, but also to the capacity of doing more with less than what others (mainly implying the United States) can afford to do. Intelligence and strategy must make them able to decrease the gap caused by technological disparity. This concern is central in the Chinese policy because the gap with the United States in terms of methods remains huge, even though the country embarked on a frantic race for the modernization of its armies. In Chinese military environments, the idea is to offset this weakness by efficiently using the methods available. This specific context guides the choices available to information warfare strategists. They must create a multi-dimensional threat and force the enemy to make cognitive errors. In order to do this, they must attack cognitive and belief systems to guide commanders' thoughts, get them to make mistakes, create strong psychological pressure using intimidation by demonstrating its capacities, using the effect of surprise mainly by creating a contrived reality, using deception, deceiving the enemy by pretending to follow his choices, developing information warfare weapons and viruses to block information flow, and using all information warfare means available to conserve information supremacy. All the ingredients for psychological warfare (psychological operations, deception), hacker warfare (viruses) and network computer warfare are there. Focusing

49 Wang B., *The Current Revolution in Military Affairs and its Impact on Asia–Pacific*, Zhongguo Junshi Kexue, Beijing, April 2000.

on "psychological" stratagems can be a dangerous choice in a real situation, because it mainly relies on the capacity to control the enemy's behavior and lead him to make errors in judgment which could be detrimental and fatal[50].

2.2.7. *2004 White Paper on national defense*

The information department of the Council of the State of China published its White Paper on the country's National Defense on 27 December 2004. The document is structured in ten chapters and focuses on the National Defense policy, the revolution in military affairs (RMA), budgets allocated to defense, system of military service, reserve and mobilization forces, challenges for science, technology and industry servicing National Defense, the relationship between armed forces and the population, cooperation in terms of international security and, finally, disarmament and non-proliferation policy.

The report does not directly discuss information warfare strategy. It is, however, important due to the fact that it presents the Chinese project in terms of defense, i.e. in the context in which the doctrine of information warfare is liable to be developed in a theoretical and pragmatic point of view.

China reaffirms the strictly peaceful character of its efforts to develop. It wishes to build a prosperous and peaceful society. China will never have expansionist ambitions and will never strive for predominant power (in reference to the United States, evidently). Its National Defense policy is strictly defensive and protects national sovereignty. There cannot be modernization and economic growth without strong security. National defense and economic developments are thus linked and must be coordinated.

---

50 As a complement to the analysis of the Chinese vision of information warfare, please refer to Yoshihara T., *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, available at: www.iwar.org.uk/iwar/resources/china/iw/chininfo.pdf, November 2001.

National security must also take into account modifications in the international environment. Large balances of power are changing internationally, characterized by a greater interdependence between governments.

Regionally, China is concerned about the role of the United States reinforcing its presence, of Japan, which is militarizing, of the Korean peninsula, representing a nuclear threat, of Taiwan, which seems to be claiming its independence and its government encouraging the population to have a hostile attitude toward China, and, finally, other threats including terrorism, separatism and extremism.

The armed forces have the power to stop the Taiwanese movement of independence, which has the potential to divide the country in two.

The RMA will be based on army mechanization and informatization. The development of information capabilities will be one of the three pillars of the RMA, with the development of fire power and mobility. In this way, naval, air and ground forces will have state-of-the-art technological methods as informatization is at the heart of this process. It must deploy military information systems, an information infrastructure, introduce ICT equipment in all operations and computerize weapon systems. As with Western military, the Chinese army will need new recruits, with a good level of education and able to use the new technologies. ICTs make it possible to intensify the integration of the different armed forces (ground, marine, air) to carry out joint campaigns and increase the efficiency of commands.

The document reminds us that the Chinese army puts a lot of emphasis on ideology and culture. Its influences are Marxism–Leninism, Mao Zedong's thoughts, and Deng Xiaoping's theories.

The army is opening up to civilian society. Industries and private high-tech companies can now participate in the military product market. The army is aware of the advantages of acquiring off-the-shelf

products, of benefiting from state-of-the-art technologies now being produced by the private sector, clearly involving information and telecommunications technologies.

The national economy must be mobilized with the army. Mobilization of the economy agrees with the concept of people's war: soldiers and people are the foundation of victory. One of the characteristics of this national economy must be its capacity to go from a state of peace to a state of war, to go from production in peacetime to wartime production. ICTs will make it possible to create a national mobilization platform for a national economy to increase the speed, coordination and efficiency of this transformation, if it ever became necessary.

2.3. Recent policies and strategies on information and cyber security

In recent months, various documents have been made public by China, agreements signed and articles published, which tell us about the political and strategic choices made in terms of cybersecurity but also of information security. In this particular case, we are interested in:

– the publication of The Science of Military Strategy[51], in December 2013[52];

– the Defense White Paper 2013;

– the Sino-Russian cybersecurity agreement of 30 April 2015;

– the PLA Daily editorial on 20 May 2015;

51 China's Science and Military Strategy, available at: https://fas.org/blogs/secrecy/2015/08/china-sms/, 2015.
Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy", *China Brief*, Washington, vol. 15, no. 8, April 2015.
52 *The Science of Military Strategy* (Chinese Version), Military Science Press, December 2013.

– the new Defense White Paper of 26 May 2015;

– the national cybersecurity law project of July 2015[53].

2.3.1. *The Science of Military Strategy 2013*

The document "Science of Military Strategy", published in 2013, was the first to devote a chapter to networked war. From this document, foreign observers can glean:

– the different categories of cyberspace operations (network reconnaissance, network defense, network attack and network deterrence)[54];

– the overall approach, the ability to involve the whole nation in cyber war (mobilization of civilian actors);

– recognition, by the Chinese authorities, of the deployment of units (PLA, Ministry of State Security and Ministry of Public Security) carrying out offensive operations – particularly testing potential adversaries' networks[55].

2.3.2. *Defense White Paper 2013*

The defense white paper published in April 2013 is entitled "The diversified employment of China's armed forces"[56].

53 An English translation of this document is available at: http://chinalawtranslate.com/cybersecuritydraft/?lang=en.

54 Franz-Stefan Gady, Why the PLA Revealed Its Secret Plans for Cyber War, available at: http://thediplomat.com/2015/03/why-the-pla-revealed-its-secret-plans-for-cyber-war/, 2015.

55 Franz-Stefan Gady, 2015, *idem*.

56 The diversified employment of China's armed forces, Information Office of the State Council, The People's Republic of China, April 2013, Beijing, 23 pages: http://aseanregionalforum.asean.org/files/library/ARF%20Defense%20White%20Papers/China-2013.pdf.

The document does not discuss information warfare and combines the concept of information with those of systems, society, infrastructure, network, sharing, dominance and "informationization" (notably announcing the reorganization of the Communications Department (in the Headquarters of the General Staff) into the Informationization Department; and highlight that the modernization of the Chinese army is gaining momentum, based on the progressive informatization, paralleling the evolution of warfare). However, there is no question of cyber (the term "cyberspace" is used only twice), but, as with other media, applying the principle: "We will not attack unless we are attacked; but we will surely counterattack if attacked"[57].

2.3.3 *Sino-Russian cybersecurity agreement 2015*

On 30 April 2015, China and Russia signed a cybersecurity agreement, also referred to by the media as the "cyber pact", laying down the principle of cooperation in the domain of international information security[58]. The agreement was signed between the respective Foreign Ministries, and was part of the cooperation treaty between the two countries (that cooperation extends to a very wide range of fields, rather than being restricted to the issues of cyber or information security), dated 16 July 2001. The agreement of 30 April 2015 states that the two countries attach a great deal of importance to the role of information and communication technologies in economic and social development, and in international peacekeeping, security and stability, and in international information security. It stresses the existence of the threat these technologies represent in the civilian and military spheres. Their use, when their purpose is to jeopardize the State's sovereignty and security, to interfere with countries' internal affairs, to violate citizens' private life, to destabilize the socio-economic environment or to stir up ethnic and religious hatred, is incompatible with the objectives of peace, security and stability. The agreement also stipulates that:

57 Page 3.

58 Russian-language version: https://www.documentcloud.org/documents/2076545-5amaccs7mslxgbff1ua785wwmwcabdjw.html English translation available at: http://www.csistech.org/blog/2015/5/11/sino-russian-cybersecurity-agreement-2015.

– the State has the sovereign right to define and implement public policies relating to information, and to telecommunication networks (the Internet);

– national cybersecurity policies can refer to the referential framework of the Shanghai Cooperation Organization;

– information security must guarantee the fundamental human rights and civil liberties. The two countries commit to ensuring information security, and creating an international information environment characterized by peace and cooperation. It is therefore necessary to create a transparent and democratic international system to regulate the Internet, to ensure equal rights of the States participating in that process, and their equitable distribution;

– this security must be developed by maintaining equilibrium between the necessary security and human rights.

The main threats (section 2 of the agreement) to international information security identified are:

– acts of aggression violating States' sovereignty, security and territorial integrity, threatening international peace, security and strategic stability;

– acts which cause economic damage, by destructive effects against the information infrastructure;

– terrorism and any act encouraging or facilitating it;

– misdemeanors and crimes, including unauthorized data access;

– interference in States' internal affairs, attacks on public order, incitement of ethnic, rational or confessional hatred, racism, xenophobia, propaganda of ideas stirring up hatred and discrimination, inciting violence, intended to destabilize the socio-economic context;

– dissemination of information attacking the political, economic and social systems, and the spiritual, moral and cultural environment.

The agreement identifies the domains of cooperation (section 3):

– establishment of communication channels and contacts to share responses to threats;

– interaction to develop and promote international judicial standards in order to assure national and international information security;

– joint responses to the threats defined in article 2;

– cooperation in police procedures (inquiries in the context of terrorist and criminal matters);

– cooperation in the area of software security of the critical information infrastructures (technology exchanges, cooperation between the respective competent authorities);

– exchanges pertaining to the legislative framework;

– support for cooperation and coordination between the two States, in the context of the international organizations and fora such as the United Nations, the ITU, the International Standardization Organization, the Shanghai Cooperation Organization Shanghai, the BRICS countries, the regional forum of the south-east Asia security association, etc.);

– encouragement of joint research, training of specialists, student exchanges; organizing conferences and meetings.

2.3.4. *PLA Daily editorial on 20 May 2015*

On 20 May 2015, the *PLA Daily*[59] published an issue on cyberspace as a sovereignty issue, mentioning the need for a new form of war. The discourse in the issue was vindictive and aggressive. The main arguments contained therein are as follows:

– the West is the enemy, because they are aggressive;

– China is under attack, ideologically and politically;

– China needs to be vigilant about the West's intentions toward it, because there have been numerous demonstrations of Western

59 http://www.81.cn/jfjbmap/content/2015-05/20/content_111375.htm.

hostility toward China. The Western (i.e. American) strategy used against China is the same as that which was employed against the USSR – a strategy of destabilization.

– China is in a stance of active defense. If attacked or threatened with attack, it is completely normal for it to defend itself.

This editorial is part of a school of thought which is critical toward the United States. Since the charging of its 5 officers, accused of cyberespionage, China has been levelling an increasing number of these criticisms at the US. The Chinese government paints the West, led by the United States, as a force for evil, capable of using the Internet to spark a revolution in China: hostile western forces, associated with a few Chinese ideological groups, have already attacked the Chinese Communist Party and denigrated its leaders, through the Internet. The Internet, it goes on, has become an ideological battleground, and whoever controls the tool will win this war; cybersecurity measures must be taken to safeguard ideological security online; the fundamental objective pursued by the West is to bring China into line with the "universal values", to upset China with a constitutional democracy, and to attack the country with a "color revolution"; the army must preserve national sovereignty and security on traditional battlefields, but also protect the ideology and ensure political security in the invisible battlefield that is the Internet.

2.3.5. *Defense White Paper of 26 May 2015*

On 26 May 2015, the government published a new Defense White Paper[60], which accorded the appropriate place to cyberspace, and to "informationization". From this point of view, China is aligning itself with the other major nations whose armies are network, computerized, use cyber technology and indeed are dependent upon it. Having acknowledged the existence of units dedicated to cyberspace, demonstrating its modernization but also defending itself against any accusation of aggression, highlighting the pacific nature of its strategy (which is known as active defense), China is bringing itself up to the

60 http://eng.mod.gov.cn/Database/WhitePapers/index.htm.

standard of the international powers: it is modernizing, creating defense forces concomitant with its rank on the international scene, and affirming that it has no intention of waging war. Cyberspace in questions of defense occupies a crucially important place. It channels ideas, ideology, facilitates influence, and is useful for destabilization. It is a space where nations must fight and impose their presence, in order to lay the foundations for future combat, or to deter potential adversaries. The logic which can be seen behind this strategy is one of occupation of spaces: on the sea, but also in space and in cyberspace (two domains which are closely linked in Chinese doctrine), we must be present. At sea, we see a strategy of expanding the range of action of the Chinese navy, and attempts at territorial appropriations (occupation of islands)[61]. The same logic can be found for cyberspace: if we do not occupy a space, somebody else will; if we do not defend our sovereign space, others will occupy it.

The main messages which we shall take from this White Paper are:

– It begins with a restatement of China's peaceful intentions, and particularly its willingness to play a role for peace in the world – i.e. to be a defensive actor beyond Chinese territory;

– the defensive strategy runs counter to any desire for hegemony, even for China itself;

– the world has multiple characteristics: it is multipolar, its economy is globalized, the information society has come into being, and overall, it is generally peaceful, though conflicts do continue;

61 China's current strategy in the oceans can be seen as the long-term implementation of Admiral Liu Huaqing's strategy (1988) of the three island chains. The hypothetical conquest would begin with a first chain, running from Southern Japan to Taiwan and the Philippines; the second from the Western Aleutians to the end of Papua New Guinea (by 2025); and by 2050, a third chain running from the Aleutian Islands to the Antarctic. The goal is to establish a presence of the Chinese navy at each of these levels (according to Jian Yang, "China's security challenges: priorities and policy implications", in *Asia Pacific Countries' Security Outlook and Its Implications for the Defense Sector*, NIDS Joint Research Series no. 5, National Institute for Defense Studies, 2010, Japan).

– in this evolving world, China is necessarily evolving, as are a number of other States which are progressing technologically and transforming their defensive capabilities;

– although the world is generally pacified, it is constantly facing threats. Thus, China is preparing for the eventuality of war, where the "computer" component is omnipresent. In line with the evolving form of war and national security situation, the basic point for PMS will be placed on winning informationized local wars, highlighting maritime military struggle and maritime PMS;

– a reform, a profound re-imagining of the operational doctrines, proves necessary, to adapt the strategy of active defense to the new context;

– this evolution of forces involves changes to the doctrine and to the form of organization. In particular, it involves the strengthening of China's capabilities and effectiveness in cyberspace – an issue which concerns all the various branches of the army. The White Paper outlines the evolutions that are needed in the PLA Air Force (PLAAF), the PLA Second Artillery Force (PLASAF), which apply, for example, to logistics or human resource management.

A section of the White Paper is dedicated to cyberspace, which is described as a new pillar of the economy, of social development, and a new area of national security. In that document, China paints itself as one of the foremost victims of cyber attacks in the world. This insecurity in cyberspace propagates into the domain of defense, justifying the establishment of cyber defense forces: "China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, support for the country's endeavors in cyberspace and participation in international cyber cooperation, so as to stem major cyber crises, ensure national network and information security, and maintain national security and social stability". The White Paper also discusses the broader project of mobilization of the population in the defense effort – particularly in the cybernetic field, via the reserve mechanism: "Improving the systems and mechanisms of national defense mobilization. China will

enhance education in national defense and boost the awareness of the general public in relation to national defense. It will continue to strengthen the building of the reserve force, optimize its structure, and increase its proportion in the PLAN, PLAAF and PLASAF as well as in combat support forces. The ways to organize and employ reserve forces will be more diversified. China will devote more efforts to science and technology in national defense mobilization, be more readily prepared for the requisition of information resources, and build specialized support forces. China aims to build a national defense mobilization system that can meet the requirements of winning informationized wars and responding to both emergencies and wars".

2.3.6. *The national cybersecurity bill of July 2015*

The document does not introduce the concept of information warfare or that of the information environment, or information operations, but focuses on cyberspace, which it links to the notions of sovereignty, governance and administration. The concept of information is tied in with security, technology, networks, identity, users, people, infrastructures and systems. The concept of cyberspace, then, seems rather to be linked to the political issues of the nation (sovereignty, governance) on the international scene.

2.4. Reflections

2.4.1. *The American perspective on Chinese information warfare, modernization and informatization of the PLA*

China perceives the strategic flexibility advocated by the United States as a wish to reinforce the American position in the Asia Pacific region, against Beijing's ambitions and claims over Taiwan.

The growth of Japanese military capacities, the increase of its fire power, added to the reinforcement of its relations with the United States in terms of security, makes Beijing believe that China has

become the object, or target, of a multilateral strategy led by the Americans in this part of the world. The Americans have reinforced their military presence close to China. In 2006, the USA planned to increase the number of American ships, aircraft carriers and submarines in the Pacific. The island of Guam was used as a station for American operations in the Pacific. Consequently, China modernized its army[62].

Unless, of course, it is the other way around: Americans reinforcing their position in view of the military emergence of China. The result, though, is the same: a tense situation and a race to weaponry.

This modernization is precisely what concerns Americans; they do not seem to understand the underlying motivation or worry about their own predominant power. The emergence of China into the ranks of global economic and military powers worries the United States. China is watched by America, and these observations are the subject of numerous reports, at least as revealing of what America thinks as they are of the situation in China.

From reading a selection of these reports, we list the major problems that have recently attracted the attention of American authorities. These reports are the Annual Congress Report "The military power of the People's Republic of China". Chinese military policy is the subject of specific observation from the Americans. In 2000, the "National Defense Authorization Act for Fiscal Year 2000" law was voted (Law no. 106-65) requiring from the Defense secretary an annual report on the military power of the People's Republic of China (Section 1202 of the law). The report must analyze the evolutions of military technological development (military, security) strategies, operations concepts and organization of armies. The reports from 2003 to 2015 were analyzed.

62 Richard A. Bitzinger, *China adapts to US defense transformation*, 11 October 2006.

2.4.1.1. *Interpretation problems*

The first problem encountered in this analysis and in any effort to understand Chinese concepts by Westerners is the cultural difference, i.e. the difference of views[63].

How can we understand a strategy, how can we figure out what words and concepts hide if we do not have the same references, the same key words? The problem is particularly crucial in terms of strategy, which, as we know, is not a simple technique that can be reduced to universal equations, but an art. And is there anything more subjective, more profoundly established in the individual, society and culture than art?

2.4.1.2. *The impenetrability of China*

China is criticized for its lack of transparency, its impenetrability, its culture of secrecy, where no one can figure out its real intentions, for example involving Taiwan, or what role China really intends to play on the international scene.

This impenetrability is a source of fear, misunderstanding and increased risks of errors in judgment, assessment and bad decisions: "The outside world has little knowledge of Chinese motivations […]. Chinese impenetrability […] will continue to make others consider the possible scenarios of conflict and to act accordingly". The impenetrability factors are:

– the policy of deception and misinformation that emanates from Beijing. This policy is associated with the traditional military notion of "shi", which uses intelligence to surprise the enemy through radical political changes and unexpected attacks. In order for this policy to succeed, priority must be given to espionage and in keeping others from collecting information on China. A war must actually be fought to collect information;

– China limits contact from foreign countries with its armies, and particularly the United States who is even pushed away from joint drills that China engages in with Russia, for example. Contact was

63 To better understand Chinese thinking, please refer to Cheng A., *La pensée en Chine aujourd'hui*, Folio essais, Gallimard, 2007.

strictly limited following the 2001 incidents on the island of Hainan. Only in 2006 links were re-established, albeit half-heartedly, between the American and Chinese armies. But the Americans estimate that these relations are unbalanced in favor of China and that care must be taken so that the American military does not divulge too much of its capacities, technologies and know-how. The United States should also reinforce its intelligence capacities;

– the consecutive reports are a reminder that there are still many unknowns on the reality of China's financial investment in this transformation. The reports denounce or confirm China's impenetrability which publishes nothing, divulges nothing involving its strategies and does not reveal real numbers or intentions.

The Americans cannot identify the real motivation behind this race to high-tech weaponry and this transformation of Chinese armies. They think the outside world has little understanding of Chinese motivations, of decision processes and key methods supporting the modernization of the Chinese army. This lack of transparency leads to legitimate questions, as the then Defense Secretary Donald Rumsfeld asked in 2005: what is the purpose of these increasing investments? The major aspects of Chinese army modernization, its goals, objectives and plans are not transparent[64]. We should certainly not pretend to believe that the Americans have no clue about China's objectives. What if the answer were as simple as so that the United States is not the only master of the world, dominating all arenas (ground, air, sea, information)? Or is it simply because China wants to have a credible army, worthy of China's ambitions? American questioning seems somewhat inappropriate. If these questions were asked, China, as well as the rest of the world, would be entitled to return the question back onto the Americans.

2.4.1.3. *Information warfare*

2.4.1.3.1. The Chinese version may only be a copy of the American version

The vision that Americans have of Chinese information warfare is not solely expressed through official reports to Congress.

64 2006 Annual Report – China Military Power.

We can cite the view expressed by James Mulvenon[65]. According to him, the Chinese approach to the concept of information warfare is a simple copy of the American model with a few minor changes, because China is unable to move away from it in an original way. The fact that China has been closely examining American experiments since the First Gulf War, but has no operational or pragmatic experience itself would partially explain this "reproduction". Mulvenon identifies the following similarities:

– the information age is described by the Chinese as the third important period in the history of humanity, following the farming era and industrial revolution. This approach is not original since it uses Alvin and Heidi Toffler's theory[66] to the letter with their famous "The Third Wave";

– the objective of information warfare is to "protect oneself and control the enemy";

– China uses the theme of info-dominance;

– China uses exactly the same pillars of information warfare defined by the US Air Force, that is to say electronic warfare, tactical deception, strategic dissuasion, propaganda warfare, psychological warfare, network computer warfare and C2 warfare;

– similarities in the idea of integrating the five dimensions of war (air, ground, sea, space, electromagnetic spectrum), principles used in the report "Joint Vision: 2010".

Mulvenon also identifies a few differences:

– for the Chinese, information warfare is a strictly military affair, whereas Westerners accept that information warfare, cyberwar, or netwar (between civilian players and governments) can all be carried out;

65 Mulvenon J., Yang R.H., *The People's Liberation Army in the Information Age*, Rand Corporation, Santa Monica, 1998.
66 Toffler A., Toffler H., *The Third Wave,* New York, Bantam, 1980.

– the Chinese resituate their discussions in their own ideological context: the Maoist guerilla strategy, the influence of the Sun Zu doctrine;

– many Chinese writings do not present information warfare as a power intensifier on the battlefield, but as an unconventional weapon of war. Information warfare is perceived as a weapon of preemption.

2.4.1.3.2. What would the objectives of Chinese information warfare be?

For the Chinese, information warfare must be used to destroy or interrupt the enemy's capacity to receive and process data. Information warfare could be used by the Chinese in a preemptive way.

The objectives of information warfare would be to destroy the opposing command system, shorten the duration of the war, minimize human losses on both sides, reinforce the efficiency of operations, reduce the effects on civilian populations and win support from the international community.

2.4.1.3.3. Capacity reinforcement of information warfare

The different reports show all the efforts, investments and progress achieved by the Chinese army in terms of information warfare capacity. They particularly identify the creation of special units. According to the Department of Defense, China has developed specialized units of information warfare and viruses to paralyze enemy systems.

The army has created information warfare units (this assertion is used by the 2007 annual report) to develop viruses to attack enemy information systems/networks, and develop tactics and measures to protect its own systems and networks. These information warfare units in the army and reserve may have been under development since at least 2000. In 2005, the Chinese army started to introduce offensive CNOs in its drills (strikes against enemy networks).

These units, made up of military personnel and civilians, could not only support the troops in their attacks, but could also carry out hacker attacks, all sorts of cyberwars against a military opponent and

commercial information systems, and help in the defense of Chinese networks. Drills are conducted to integrate the information warfare units in regular military operations. This information echoes articles published in the Chinese press.

2.4.1.3.4. What would Chinese targets be?

In the annual report to Congress "US–China Economic and Security Review Commission's Report 2006", information warfare is a series of unconventional military methods.

China wants to exploit vulnerabilities caused by the United States' dependence on these technologies. It wants to acquire C4ISR systems to be able to paralyze those of the adversary (a C4ISR architecture makes it possible to coordinate forces in all four dimensions – air, ground, space and sea – to locate, follow and aim at the enemy). Information warfare targets are military and civilian without distinction.

The United States is vulnerable to attacks, as demonstrated by the Titan Rain operation. In August and September 2006, attacks against the information systems of the Bureau of Industry and Security of the Department of Commerce led to the replacement of hundreds of computers and to the blocking of Internet access for close to a month.

China's objectives, which do not justify the transformation of its armies with budgets allocated to defense in exponential growth, can hide medium- and long-term strategies that Americans seem to have a hard time predicting. Among the strategies considered, wars conducted in the information sphere must not be ignored.

2.4.1.3.5. What information warfare attack is China preparing?

Attacks would target enemy C2s, communication systems and the transmission of precision weapon information, which are the first instruments of the modern American war.

China wants to acquire and exploit knowledge created by others and must fight a war for the acquisition of information. To reach this objective, intelligence is a major tool and China has institutionalized the practice:

– there are 2–3,000 spy companies (real or assumed) in operation in the United States[67];

– Chinese students and residents can transmit information to China;

– economic intelligence is used.

With the use of asymmetric weapons, China would want to deteriorate enemy C4ISRs and use anti-satellite weapons, CNAs, the introduction of viruses and massive hacking. Consecutive reports highlight that China has the necessary capabilities to attack C4ISRs. CNAs are an inexpensive and efficient way to fight against a stronger enemy; they are considered to be long-range weapons. The Chinese would favor attacks against weak points, the most vulnerable and accessible networks used to exchange unclassified information, instead of first attacking highly protected secure networks. China has considerably expanded its information operations during the last few years, reaching such a level that it is clearly designed to attack American systems.

The Annual Report to Congress "The Military Power of the People's Republic of China 2007" emphasized the conceptual knowledge of information warfare by the Chinese and quotes a text published in the *Liberation Army Daily* in November 2006: "The mechanism to take control of the enemy in a war under informatization[68] conditions finds its strongest expression in our capacity or not to use several methods to obtain and ensure efficient circulation of information, our capacity or not to fully use permeability, sharing property and connection of information to achieve organic fusion of materials, energy and information in order to create a combined combat force, and in our capacity or not to use

67 Refer to the articles: *3,500 Chinese spy companies identified in Canada and the USA*, 8 August 2003, Asian Pacific News service, available at: http://www.primetimecrime.com/APNS/20030808chinesespy.htm, and *More claims of Chinese spying emerge*, 6 July 2005, Australian Broadcasting Corporation, TV Program Transcript, Reporter Tony Jones, available at: http://www.abc.net.au/lateline/content/2005/s1408571.htm.

68 See WANG B., *New Military Revolution in the World, Subduing Enemy Force without Battle, Informationized Warfare*, Zhongguo Junshi Kexue, Beijing, May 1999.

efficient methods to weaken superiority of information of the enemy and the operations efficiency of enemy computer equipment".

CNOs include CNA, CND and CNE and are an integral part of the policy of modernization of Chinese armies. The army considers CNOs as particularly critical for taking the initiative and acquiring electromagnetic dominance as soon as possible in a conflict, and as a power intensifier. We have no knowledge of Chinese CNO doctrine, but Chinese thinkers speak of "integrated network electronic warfare", highlighting the integrated use of electronic warfare, CNOs, and limited kinetic strikes against C4 nodes to interrupt the enemy's information system networks on the battlefield[69].

2.4.1.3.6. The acquisition of information warfare technologies

The Chinese army invests in electronic counter measures, defense against electronic attacks and CNO (CNA, CND, CNE) methods to dominate the electromagnetic spectrum early on in any conflict. Chinese thinkers speak of an "integrated electronic warfare network" to call for the use of electronic warfare, CNOs and kinetic strikes to destroy the information systems of the battlefield.

China continues its foreign acquisition of (notably dual) technology investments, useful to the development of computerized network centric forces: software, integrated circuits, computers, electronics, semi-conductors, telecommunications, and information security systems.

The Americans denounce the efforts of China to acquire, legally or not, dual technologies through commercial exchanges and agreements, or even joint ventures, particularly with software and integrated circuit manufacturers, at the heart of the requirements to fight network centric warfare and information warfare.

China grants large investments to acquire asymmetric military capacities (cyber warfare and electronic warfare capabilities).

---

69 For more information on the digital battlefield, refer to Yuan B., *On IW, Digital Battlefields*, Zhongguo Junshi Kexue, Beijing, February 1999.

China is not settling for just acquiring. It also provides weapons to sensitive countries like Iran, Burma and Sudan. This development at any cost, despite international rules, is what concerns the Americans.

2.4.1.3.7. The role of nationalist hackers or hacktivists

The Congress report "Annual Report on the Military Power of the People's Republic of China 2003" recalls the dangers inherent to nationalist hacking (hacktivism) in periods of tension or crisis. The increasing presence of China over the Internet and the application of the people's war principle to network warfare constitute serious threats for American networks that may be the target of massive attacks.

In light of the current and future potential of Chinese Internet users, the relative proportion of attackers is reason for concern. The role of the Chinese government must be significant. Would it support hacktivism or would it not? Although the report does not further discuss these hacktivists, the media provides numerous examples.

Recently, incidents and political events perceived as threats to Chinese integrity and national sovereignty, and the identification of major adversaries, triggered massive cyber attacks from hackers wanting to defend the interests of China:

– bombing of the embassy of China by NATO forces in Belgrade on 8 May 1999 led to a series of attacks (DoS, massive email transmissions, viruses and intrusions) against American sites. We are speaking here of a Chinese–American cyberwar. The Chinese Liberation Army newspaper, on 27 July 1999, wrote that a network battle was being fought between China and the United States;

– battles in the form of duels between hackers (site defacements, data stealing, viruses) were launched following a speech from the President of Taiwan, Teng-Hui Li, in August 1999, declaring the "two States" principle;

– in 2001, the United States was the victim of a legitimate attack against its official websites as a protest for the death of a Chinese pilot, Wang Wei, during a collision with an American spy plane near the Chinese coast on April 1st. Chinese hackers, including Honker

Union of China (HUC) and Chinese Red Guest Network Security Technology Alliance, organized massive cyber attack campaigns during the month of April; close to 1,200 sites were affected by DoS attacks including the White House and the US Air Force[70]. Did the Chinese government sanction those attacks? Were these attacks condemned publicly? During these battles via the intermediary of computers, the USA was clearly not out done because a group of American hackers, called PoizonBox, is thought to have defaced around 100 Chinese websites at this time;

– from 2003, the exiled Tibetan government in India has been accusing groups based in Beijing of intruding on its official sites and spying. Hackers send emails containing Trojan horses with legitimate-sounding addresses to make them seem more authentic;

– in 2003, the Taiwanese government accused Chinese military hackers of launching several attacks against its information systems. But were they military or hacktivists?

– hundreds of South Korean government computers were infected during the last months of 2003 by viruses capable of stealing passwords and other sensitive information. According to KISA (Korean Information Security Agency), during the first six months of 2004, a total of 10,628 hacking cases were recorded, which is 30 times higher than in the same period in 2003;

– in April 2005, Japan was faced with strong anti-Japanese sentiment, translated by violent street manifestations in Beijing and Shanghai, with some military personnel even calling for war. The tensions were accompanied by a resurgence of "cyber attacks" against Japanese websites: embassy sites, national agencies, ministry of Defense, of Foreign affairs, universities and corporations.

Who are these patriot hackers whose actions are simultaneously the illustration of the "people's war" concept and a method of "active defense"? Are they a reply to external attacks, threats to enemy systems, or protection of the country's own systems? They target

70 For more information of the Chinese attack campaign of April 2001, the readers can refer to a series of articles at http://strategique.free.fr/archives/textes/ca/archives_ca_14.htm.

research centers, corporations and government departments in all industrialized countries. The attacks have many goals including information theft, espionage, ideological demands and destabilization. It is very difficult to demonstrate the involvement of authorities in these actions that we credit to cyber criminality, or organized groups of hackers. This is especially true when we can demonstrate with certainty that they come from China and that the parties responsible are actually Chinese.

2.4.1.3.8. Can the United States remain a victim without reacting?

The potential Chinese threat raises awareness. In its annual report of 2005, the US–China Economic and Security Review Commission recommends that Congress mandate an investigation conducted by the appropriate agencies, involving cyber attacks against American networks from China.

If it can be proven that China is responsible for these attacks, that it is an accomplice or that, because of negligence, it lets its citizens attack networks, then, insofar as these threats constitute hostile acts against the United States, Congress could ask the President to advise on the measures to take against China, in accordance with current laws, or ask that measures be taken to discourage attacks against American networks.

2.4.1.3.9. Why is China intensifying the modernization of its armies?

China has long been a weak country in terms of its military. But its economic growth since the 1990s has provided the means to invest in its defense. China's defense budget is now the second largest in the world after the United States, albeit far behind in absolute value[71].

This budget continues to grow every year in an impressive way. What is China looking for with this military growth? Does it simply want to be able to promote an image as a credible military force to the world?

---

71 For more information of the strategic power of China, refer to Lim T.W., *Analysis of China's Strategic Power*, Singapore Institute of International Affairs (SIAA), 8 December 2002.

Reinforcement of the technological military capabilities serves the strategic interests and political intentions of the country well in the Asia-Pacific zone, notably preparing the country to fight and win a short-term and high intensity conflict against Taiwan, with the United States or any other country that would come to the rescue of the island.

To the Americans, China cultivates ambiguity while modernizing its armed forces. When it conducts ballistic missile tests over the Taiwan Strait, it maintains that it has no aggressive designs against Taipei and calls for a peaceful reunification.

2.4.1.3.10. Preparing for new wars?

The Desert Storm operation resulted in the modernization of C4ISR systems and the development of information warfare, precision weapons and logistic capabilities.

The Allied Forces operation (1999) had a similar impact on the Chinese army thought process, confirming the first conclusions of the necessity of preparing for new wars, notably by observing how the Serbs could resist with technically inferior methods against the American attacker. The “three attacks, three defenses” principle is the direct result of these observations and conclusions of the Allied Forces operation; attack by aviation, cruise missiles, helicopters; defense against precision fire, electronic warfare and enemy reconnaissance.

2.4.1.3.11. Arriving in the information age

Military modernization is, then, based on a finite analysis of American military operations since the 1990s (American operations in Iraq in 1991 and 2003 and in Kosovo in 1999). The Gulf War of 1991 showed that an army built around technologies and methods inherited from the Soviet army was doomed to fail against the power of a modern military such as the United States, made possible because of its RMA based on technological progress.

Chinese priorities include reaching the information age, introducing and adopting technologies and information tools as well as solutions for increased mobility and precision strikes. Marine,

ground and air forces are all benefiting from the major investments granted by the government.

The Chinese army's transformation is guided by the objectives of being able to fight and win a "limited local war under conditions of informatization" and modernizing an army that has long been guided by the "people's war" principle dear to Mao Zedong. This new doctrine means engaging in short and high intensity conflicts, characterized by mobility, speed, long distance attacks occupying all spaces simultaneously; ground, air, sea, space, electromagnetic field and field of information rely on very deadly high-tech weapons (unconcerned about reducing human losses, or at least not focusing on the question like the United States does with its obsession with zero death).

2.4.1.3.12. Ambitions beyond Asia-Pacific?

The annual report to Congress "The Military Power of the People's Republic of China 2007"[72] states the concern of the United States with the increase in power of the Chinese army whose technological developments and profound transformation cannot be justified only by a possible conflict in the Strait of Taiwan.

According to the same report:

– the Chinese army has great potential to confront the United States and engage in regional conflicts for resources or territory. The growth of China's military capabilities clearly has implications that go beyond the Asia-Pacific region. The strategy of banning access and the protection of air, sea and ground territories clearly expands to space and cyberspace. The report again uses the notion of China's "lack of transparency" involving its objectives and the very limited knowledge of the West about these objectives and China's motivations;

– the development of China is presented as being particularly aggressive. Any means seem acceptable to reinforce its civilian and military industry, and the boundary between the two is very small

72 http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf.

since civilian industry is at the service of national security. China must grow technologically and acquire as many technologies and as much know-how as possible, and very quickly, to feed its economy, progress and modernization (especially of its armies). The Americans see the practice of economic intelligence in the Western and Japanese model (officially encouraged by the Chinese government) as illicit practices, bordering on espionage. This battle for the acquisition of strategic and technological information also involves infringing on intellectual property rights (copying of patents, breach of industrial secrets, reverse engineering). The programs for science and technology are based on the assimilation of foreign sciences and technologies, and the civilian–military relation is at the heart of these developments.

2.4.1.3.13. In search of interpretations: the concept of "shashoujian"

"Shashoujian", which can be translated as "assassin's mace", is a relatively common expression in China, expressing the means and methods by which it is possible to overcome a seemingly insurmountable obstacle. This involves an action or a quality, offering a strategic advantage, when it is used for a specific purpose, in a particular manner and at a specific time[73].

The term appeared in the annual "US–China Security Review Commission Report 2002", then used again in the annual reports to Congress "Military Power of the People's Republic of China" of 2004 and 2005. It certainly intrigued American observers, who immediately saw a new mystery in contemporary Chinese strategic thinking and it therefore had to be decoded as soon as possible. The American Department of Defense claimed that China intensively pursued the development and acquisition of asymmetric "assassin's mace"-type solutions, recognizing at the same time its inability to say with precision if this term indicated specific technologies, concepts or a strategy.

73 Also read Johnston A.L., *Toward Contextualizing the Concept of a Shashoujian (Assassin's Mace)*, Government Department, Harvard University, August 2002.

The term is not recent (it is thought to date back to the Tang period) but it has reemerged recently in the context of debates involving the modernization of Chinese armies in the middle of the 1990s, after China became really aware of its backwardness compared to the undeniable technological superiority of the Americans. The term is used to describe a secret weapon, a platform, a dissuasive system or a tool helping to reach a political/psychological/military victory with a single decisive, fatal battle. The military concept of "shashoujian" cannot be reduced to the idea of a "magic" weapon, to the concept of *Blitzkrieg* or to the idea of launching an abrupt and total attack (an electronic Pearl Harbor, for instance) that would make it possible to paralyze an enemy before even starting a war. The concept of "shashoujian" focuses more on the capabilities of the "inferior" enemy in an asymmetric conflict, the possibility for that enemy to win the war despite its inferiority.

Why has the term come back in the military world? When the Taiwanese President Lee Teng-Hui wanted to confirm the position of Taiwan in relation to Beijing, China replied with a demonstration of force by firing ballistic missiles off the Taiwanese coast. The United States reacted immediately by sending a fleet in a show of support for Taiwan. President Jiang Zemin then asked his army what possibilities there were. The response was: "Nothing!". Politically powerless against the United States, the Chinese government has since strived to develop new capabilities enabling it to one day force its will. Chinese capabilities are and will remain for a long time inferior to the United States, but they need to find a way to take advantage of such a situation that is *a priori* unfavorable, which would be possible with an "assassin's mace", enabling it to win in the Taiwan Strait in an asymmetric situation. This "shashoujian" is therefore mainly a general principle, an idea, a concept, more than a specific technology. That is what will make China able to impose itself on a more powerful enemy, for example by making an American intervention useless, too costly and/or too risky. "Shashoujian" could consist of a diplomatic opportunity, a strategic manoeuver, the use of speed (a long-range missile strike that American ships would not have time to detect), or the use of submarines, computer network attacks, communications satellite attacks and information warfare to deteriorate American

C4ISR systems, the effect of surprise in taking a military advantage and pursuing through diplomacy, running the risk of a generalized conflict which the United States would not want to engage in. We can imagine solutions and different configurations. The only option available to China at present is to prepare for asymmetric conflicts if it finds itself at war with the great powers.

What are the expected effects of "shashoujian" type strikes?

– *Dissuasion*. This is the equivalent of the Sun Tzu formula: "Winning without fighting". Today, ballistic missiles and submarines are considered shashoujian type forces used as the basis of psychological warfare;

– *Decapitation*. i.e. killing the enemy in one clear and fatal shot. That is the ideal goal;

– *Blinding, paralyzing, disintegrating*. It is the acupuncture war (*dianxue zhan*) that must have systemic effects on enemy structure and military organization. Chinese strategists discuss the importance of shashoujian strikes on critical infrastructures: C2 centers, networks, intelligence systems, sensor platforms and military logistic systems. Such systems are taken as a source of weakness of the superior enemy, more vulnerable to attacks. Attacking weak points, and especially vital points, paralyzes the adversary and then initiates the disintegration of a superior force.

2.4.1.4. *2008 DoD report concerning Chinese military power*

In March 2008, the United States Department of Defense published its annual report on the military power of the People's Republic of China[74]. The report insists once more on the concerning development of seemingly aggressive military capacities and doctrines and strategies in China. China, which has become a vital partner internationally, still represents a serious threat to peace in the world. The report questions once more the place that information warfare has in the constitution of this "Chinese threat". But could the report be revealing American perceptions, psychology or strategy instead of

74 The report can be downloaded in full at http://www.defenselink.mil/pubs/pdfs/China_Military_Report_08.pdf.

being a strictly objective description of the Chinese reality that it wants to conquer?

The 2008 report has seven chapters, with a summary, a glossary of acronyms and appendices:

– Chapter 1: Key developments.

– Chapter 2: Understanding China's strategy.

– Chapter 3: China's military strategy and doctrine.

– Chapter 4: Force modernization goals and trends.

– Chapter 5: Resources for force modernization.

– Chapter 6: Force modernization and security in the Taiwan Strait.

– A chapter dedicated to human capital in the PLA modernization.

– Appendices proposing a series of quantitative data on the military forces of China and Taiwan.

As an introduction, the report highlights the major role that China now plays on the international scene, achieved through the unconditional support of the United States: "No country has done more [than the United States] to assist, facilitate and encourage China's national development and its integration in the international system"[75]. Uncertainties surround the course chosen by China however: what is the purpose of the expansion of the Chinese military power, and how will this power be used?

The new China–United States, China–Asia, China–rest of the world balances of power are quickly becoming the major subject. On the one side, there is the United States with peaceful intentions, and on the other, China, seemingly peaceful but suspected of not remaining that way, of wanting to switch from simply ensuring its defense to an aggressive player, preparing local wars[76] with the help of high-tech

75 Page 1 of the 2008 report.

76 To defend territories where China claims sovereignty, and for the "One China" principle to be respected: territories include Taiwan, the Paracel and Spratly islands, islands in the South China seas, etc. These territories are claimed by many countries

resources ("local wars under conditions of informatization")[77] and able to confront the United States in a military context (this idea taken from the 2006 Quadrennial Defense Review Report[78]). According to the United States, China is preparing for the possibility of a conflict in the Taiwan Strait, including in case of American intervention. In order to quickly modernize its armies and achieve its RMA[79], China has agreed to significant efforts and investments: acquisition of state-of-the-art weapons, notably from foreign countries, modernization of its nuclear arsenal, development of a strong technological and scientific industry, and reformulation of its doctrines, thus affecting the army organization to its core.

Chinese doctrine is perceived as a free mix of ancient and modern sources, including strategists of the era of Imperial China and Chinese Communist Party icons. This multitude of sources is the reason why Westerners do not understand China, and because of this, the study of Chinese military strategy remains a fundamentally inaccurate science. This comment is surprising: is there an army with a history that is not today built on both the past and the present? The report identifies a few "concepts" deemed vital to the understanding of Chinese action today and in the future.

2.4.1.4.1. The 24-character strategy

"Calmly observe, secure the position, face the events with calm, hide our capacities and wait for the right moment, try to maintain a low profile, and never claim leadership". This sentence, written in 24 Chinese characters and attributed to Deng Xiaoping was used as a guide for the Chinese system of foreign affairs and security policy

---

in the region: Brunei, the Philippines, Malaysia, Vietnam, Russia, Japan, India, etc. For a map of territorial conflicts, see page 11 of the 2008 report.

77 "Informatization" here means operation environments characterized by the jamming of communications, electronic surveillance, and precision weapons.

78 2006 Quadrennial Defense Review Report: "China has the greatest potential to compete militarily with the United States". Downloadable report at http://www.comw.org/qdr/qdr2006.pdf.

79 Abbreviation of Revolution in Military Affairs. The expression represents the process of modernization of armies in the context of a technological revolution.

early in the 1990s. Some elements of this strategy continue to be used by the heads of Chinese security in the context of diplomatic and military affairs. This strategy is instructive in that it suggests maximizing the options to come without useless provocations. The Americans see in this concept one of the keys for interpreting Chinese attitudes internationally[80].

2.4.1.4.2.The Chinese opportunism

Chinese leaders have described the first 20 years of the 21st Century as a period of opportunity[81], providing peaceful regional and international conditions, and conducive for China to dominate regionally and have a global influence. This means that during this period of opportunities, the country must be able to seize its chances; every occasion should be used for its benefit. Opportunism does not mean simply waiting for change, however. It can involve frequent changes of policy, tactics and economics, according to the context. Opportunism involves a strong capacity to react and to adapt. Opportunism is often considered as an attitude that ignores moral principles. Should we increase political and economic influence at any cost? Should we be able to abandon political or ideological principles considered as fundamental to expand our political influence? How can these opportunities materialize: through alliances, collaboration agreements, by exploiting the weaknesses of other nations, by organizing the exploitation of all the flaws of the international system and, if so, then why not include the information systems that we know are so fragile? But opportunism is not without risk. As early as 1928, Leon Trotsky, writing about the Chinese revolution involving the "classic mistakes of opportunism", mentioned the risks that ideological movements take when they sink into opportunism[82].

---

80 Medeiros E.S., "China's international behavior: activism, opportunism and diversification", *Joint Force Quarterly*, issue 47, 4th quarter, 2007, pages 34–41. USA. Available at http://www.ndu.edu/inss/Press/jfq_pages/editions/i47/8.pdf.

81 Chapter 2, page 9 of the 2008 report.

82 http://www.zhongguo.org/trotsky/revbetrayed/images/China/27.htm "Leon Trotsky on China. The classic mistakes of opportunism" January 1928.

2.4.1.4.3. Asymmetric war and the concept of "shashoujian"

The report uses the famous concept of the "assassin's mace" ("shashoujian" in Chinese)[83]. It appeared in the annual report "US–China Security Review Commission Report 2002", and was used again in the 2004 and 2005 annual reports to Congress "Military Power of the People's Republic of China". The term was intriguing for American observers who immediately saw a new mystery in contemporary Chinese strategic thinking. The 2008 report goes back once more to this concept, defining "shashoujian" programs as an integral part of the Chinese asymmetric war strategy, giving a technologically inferior party military advantages over technologically superior adversaries, in order to change the direction of the war. The descriptions of the use and effects of "shashoujian" type platforms are compliant with the Chinese asymmetric war strategy and mainly consist in the integration of modern and older technologies used in an innovative way. Would cyber aggressions carried out in peacetime come from the preparation of these solutions, by providing a player with the flaws of potential adversaries? Regardless of the solutions being developed, American intelligence estimates that China will have to wait at least 10 years before having a modern army able to beat a medium-sized adversary[84].

2.4.1.4.4. Place of the "information warfare" concept in the report

The concept of "information warfare" is addressed in its own section within the 4th chapter on the objectives of army modernization. The terms of the report remain vague, simply indicating that military strategists have a deep understanding of the concept, its methods and uses. Text from a Chinese report published in the *Liberation Army Daily* review[85] in November 2006 defines the concept of information warfare. This quotation, already present in the 2007 DoD Report, does not provide any new information for identifying a specifically Chinese approach to the concept. Information warfare is "the mechanism to take control of the enemy in a war under informatization conditions, which finds its strongest

83 See page 20 from the 2008 report.
84 See Chapter 4, page 22, of the 2008 report.
85 http://www.pladaily.com.cn/.

expression in our capacity or not to use several methods to obtain and ensure efficient circulation of information, our capacity or not to fully use permeability, sharing property and connection of information to achieve organic fusion of materials, energy and information, in order to create a combined combat force, and in our capacity or not to use efficient methods to weaken superiority of information of the enemy and the operations efficiency of the enemy computer equipment".

Data relative to investments is then provided, but without a statistical approach. It simply states, as in previous reports, that the Chinese army invests (in acquisition or development?) in methods of electronic counter-measures, defense against electronic attacks (angle type reflectors, false target generators) and CNO (Computer Network Operations)[86] to dominate the electromagnetic spectrum early in the conflict.

The report mentions the creation of special units of information warfare in China. According to the Department of Defense, China has integrated specialized units of information warfare and developed viruses to paralyze enemy systems. But again, this is information already published in previous Department of Defense reports.

No information relative to information warfare in the 2008 report is any different from the contents of the previous reports. Does this mean that intelligence departments have nothing new to add to the report about this subject? Or would it mean that the subject may have been put somewhat aside to concentrate on other objects of concern like the tension in the Taiwan Strait, the development of human potential or the arsenal of ballistic missiles? Would information on information warfare not offer sufficiently interesting arguments to feed the image of the "Chinese threat"? Even though several countries brought accusations against the Chinese army in 2007 involving aggressions against government information systems, nothing in this chapter establishes any link between the events and the PLA; there is no constructive comment to agree with the accusations or to contradict them. The report is of no help in better understanding the Chinese

86 This military concept from American doctrine groups CNA, CND and CNE.

doctrine and strategy in terms of information warfare, which appears not to have changed in the last few years.

2.4.1.4.5. Cyberwar methods

By "cyberwar" the Americans mean confrontations in networks, hacker wars conducted by the military. Non-military hacker warfare, confrontations between hacktivists and aggressive maneuvers in cyberspace by non-military entities is covered in the concept of "netwar", not discussed in this report. In Chapter 1 ("Key developments"[87]), there is a section dedicated to cyberwar methods. During 2007, several attacks against computer networks occurred around the world, including the information systems of the United States government, victims of intrusions that seem to come from continental China. These intrusions would require significant skills and means. The report recognizes that there is no certainty that these intrusions were led by, or with the support of, the Chinese army or other Chinese government elements. It does maintain, however, that the development of cyberwar capacities is compliant with the doctrines published by the Chinese army on this subject. Some of the now famous incidents of 2007 include:

– the Department of Defense and other agencies or departments of the United States government, as well as contractors or think tanks linked to defense, were the targets of several intrusions in their systems, and many of them seemed to come from continental China;

– the Vice-president of the German Intelligence Department, Hans Elmar Remberg, publicly accused China of supporting daily intrusions in information systems. These intrusions were suspected to be for the purpose of stealing information so that China can catch up technologically as soon as possible;

– in September 2007, the French Secretary General for national defense confirmed that the government's information systems were the target of attacks from China;

87 Pages 3 and 4 of the 2008 report.

– aggressions seeming to come from China affected British companies, and the CEO of MI5 alerted 300 financial institutions in the country of risks of aggression from China.

2.4.1.4.6. From cyberwar to espionage

No revelations or any new information can be found from reading the press or from the numerous articles on the Internet, and the American intelligence services did not add to the 2008 report with respect to Chinese involvement.

On the other hand, even though mention of the facts is preceded by a short sentence giving China the benefit of the doubt (because it is technically impossible to identify with certainty the authors of these acts, and it is unclear if these intrusions were conducted by, or with the endorsement of, the PLA or other elements of the PRC government), the whole section can be understood as a clear denunciation of China.

The actions are attributed to China, whether guilty or innocent. The motives of these attacks do not seem to have been the subject of a deeper analysis, as they are presented as obvious. Economic espionage is the only argument that can be proposed, because of the nature of targets affected or attempted. China wants to quickly access high technologies. The Federal Bureau of Investigation (FBI)[88] and the Immigration and Customs Enforcement (ICE)[89] have named China as a major threat in terms of espionage against the United States. In the last few years, we have seen an increase in investigations involving illicit weapon and technology exports to China. As with the cyber aggressions of 2007, the report provides examples:

– in December 2007 a resident of California was sentenced to two years in prison for his involvement in illegal export activities of night vision technologies to China;

– the ex-director of a research institute linked to the Russian space agency was sentenced to 11 years in prison for having transmitted classified technologies to China.

88 http://www.fbi.gov/.
89 http://www.ice.gov/.

This economic espionage seems to be caused by the Chinese army and government because accusing fingers have declared them as being at the origin of the 2007 attacks. The report is not meant to propose interpretations. Some questions should be raised, however. Is espionage the only reason for the attacks against information systems? Is China the only possible source? Can other motives explain acts of aggression, such as target observation, implementation of tactics and aggressive operation methods, with the purpose of more ambitious actions in the future or to demonstrate power? Different hypotheses are completely ignored in this report.

2.4.1.4.7. The military doctrine: the duality of the Chinese strategy

The few lines dedicated to the recent developments of the Chinese military doctrine do not identify any major evolution of the information warfare concept. Only the firm directives instructing the armies to train in computerized environments and integrate leading edge technologies in their structures are mentioned. The fundamental texts have remained essentially the same since 1993, reflecting the impact that the 1991 Gulf War had on military doctrines. However, it seems that today China is shifting from "developing" its forces consisting in preparing them for modern wars, to wars in the information age, to training for "winning" these wars[90]. The strategy remains active defense, consisting in not engaging in a war of aggression, but only engaging in defense wars for national sovereignty and territory integrity. Once hostilities have started, the essence of active defense is to take initiative and annihilate the enemy. But the definition of the attack against the sovereignty of China remains vague. Preemptive actions have been conducted in the name of the defense strategy; for example, China's interventions during the Korean war (1950–1953) to help Korea resist against the United States. The actions carried out during border conflicts are presented as self-defense counter-attacks. The idea is to protect interests perceived as central by China through actions that may be preemptive, preventive, coercive, etc. Striking after the enemy strikes does not mean passively waiting for the enemy to use force. This Chinese strategy thus justifies offensive military actions (said to be preemptive)

90 Chapter 3, page 16 of the 2008 report.

at operational and tactical levels, under the pretense of a strategic defensive posture. Finally, the Chinese military doctrine clarifies that an enemy strike is not limited to conventional kinetic military operations. An enemy strike can also be defined in political terms. Could the reasoning be taken further? By supposing that the cyber-aggressions encountered by a large number of countries in 2007 were in fact Chinese, would they be part of these operational and tactical offensive actions justified by a defense strategy? Could the 2007 aggressions be a form of defensive reaction? Is China's informational space a domain of sovereignty that the government is ready to defend based on the same arguments and strategies that it uses for its territorial conflicts with neighboring countries? Why then, if that is the case, would China not have claimed responsibility for these actions?

2.4.1.4.8. The capacities of anti-access/area denial capabilities

This concept[91] captures the attention of the report's writers. The strategy consists of creating an insurmountable zone for anyone who would want to penetrate it in the context of the preparation of a confrontation with Taiwan, and is mainly based on the deployment of a nuclear arsenal, ballistic missiles, or even anti-satellite weapons. It involves ground, sea and air dimensions. This strategy would now extend to cyberspace[92] and consist of information control (dominance of information). China is developing operations security, electronic warfare, information warfare and deception solutions. Information dominance involves using civilian and military power instruments in all dimensions of the modern combat space[93].

2.4.1.4.9. Cartographic absence of information warfare resources

The report proposes 17 illustrations (diagrams, figures) relative to:

---

91 See also Cliff R., Burles M., Chase M.S., Eaton D. and Pollpeter K.L,. *Entering the Dragon's Lair: Chinese Anti-access Strategies and Their Implications for the United States*. RAND Project Air Force, 155 pp., 2007. http://www. rand.org/ pubs/monographs/2007/RAND_MG524.pdf.

92 Chapter 4, page 22 of the 2008 report.

93 Chapter 4, page 24 of the 2008 report.

– the space of Chinese military influence (territories that are subject to dispute, the extent of maritime power and the range of ballistic missiles)[94];

– army potential in terms of equipment (conventional and ballistic missiles)[95], investments (defense budget)[96], and efforts in the development of a modern system by force (ground, air, sea, space)[97];

– the balance of power in the Taiwan Strait, in ground, air and naval forces[98].

Several sections in the report are dedicated to the doctrines and methods underlying Chinese information operations. However, capacities in terms of information and communication technologies for military use, and in terms of resources allocated to information warfare, are not listed. No table or diagram presents the respective potentials of continental China and Taiwan in terms of information warfare resources (location or number of cyber units integrated to armies, scope of deployed C4ISR systems, inventory of informational weapons, etc.). And yet, the information space is now perceived by the United States as a field in itself, in the same way as the more traditional arenas (ground, air, sea, space). Maps of that space would be interesting but, in the absence of maps showing Chinese information warfare resources, we can attempt to advance some explanation:

– either these resources do not exist (highly unlikely);

– or they do exist but are not significant and do not deserve to be represented. This second option would put into question all the theories put forward by the series of reports on the Chinese military power published by the DoD since 2002;

– or the resources exist but their location, measurement and identification are impossible. By their nature, they do not lend themselves to statistics. It is easier to count the number of nuclear

94 Figures 1, 2 and 3 of the 2008 report.
95 Figures 4 and 5 of the 2008 report.
96 Figures 6 and 7 of the 2008 report.
97 Page 8 of the 2008 report.
98 Figures 9 to 17 of the 2008 report.

warheads than informational weapons. We must find other units of measurement;

– or again, these resources are identified but the Americans do not wish to show them, either because they want to keep their knowledge confidential, or because they prefer to focus the report on other themes.

2.4.1.4.10. Objective portrait of China or reflection of American opinion?

One of the characteristics of this report, which is an attempt at painting a picture, remains the admission of being unable to complete it; "the international community has limited knowledge of the motivations, decision-making, and key capabilities supporting China's military modernization"[99]. Doubts, unknowns and uncertainties are important variables of this report. Several times, the text emphasizes the absence of knowledge, lack of vision, the difficulty in understanding Chinese thinking, its objectives and its strategies. This is obviously not presented as a lack of information based on American flaws, but as the problem with China's communication of information, explanations, openness and clarification; "China continues to promulgate incomplete defense expenditure figures". The report again denounces the "lack of transparency" of Chinese affairs, a source of risk for stability and presents China as a player who conceals, who lacks sincerity. China continues to "engage in actions that appear inconsistent with its declaratory policies"[100], "less clear are the specific strategies and plans Beijing has developed to achieve these objectives"[101], etc. There are many unknowns in the eyes of the Americans.

In Chapter 2 of the report, the authors write "China's leaders have not publicly articulated an explicit, overarching 'grand strategy' that outlines national strategic objectives and the means to achieve them […]. Although such vagueness may reflect a deliberate effort to conceal intentions and capabilities, as implied in Deng Xiaoping's

99 Page 1 of the 2008 report.
100 Ibid.
101 Chapter 2, page 9 of the 2008 report.

‘24-character strategy’… it may reflect […] disagreements and debates among China’s leaders”[102].

It appears impossible to trust a speaker, who is not really a speaker, if they lie, conceal, hide the truth. China is portrayed as an underhanded menace threatening the rest of the world. The United States appears as a legitimate informer, justice of the peace, guarantor of balances. The vision of the world remains divided; what is not understood, seen, heard, shown or said is obviously suspect. On one side there is truth. On the other side, there is lying, a “lack of transparency”, the adversary that we make up. Denouncing ambiguity, duality and opacity is confirmation that China has secrets to hide: we remember the inventory of chemical weapons hidden in Iraq which was the argument that served in part to justify the military intervention in that country. Accusing a party of lying and concealing in a security context makes the adversary a threat and demonizes it.

Is the “Chinese threat“ a real threat or is it mainly an intellectual construction? Where is the reality in the description made by the report? And is not the description of this reality written under the influence of what we might call an American feeling of insecurity? China has for centuries been the subject of great fascination. It is today presented as both:

– attractive:

- mainly commercial interests,

- cultural attractions;

– source of risk and threats:

- because of its political regime, survivor of the communist era and awakening cold war fears (of a nuclear threat),

- because of its growing power that no one knows the limits of (competitive supremacy with the United States?),

- challenging the world balance centered until now, in financial, political, military and cultural terms, on the role of the United States,

102 Chapter 2, page 8 of the 2008 report.

- challenging the future of the planet: a nuclear power, a polluting power, etc.

Is China, first and foremost, a strategic threat to the United States or a commercial godsend? In dealing with China, should we collaborate or confront? In fact, which conjunction is more relevant here: "or" or "and"? Shouldn't the questions be reformulated as "Is China a strategic threat and a commercial godsend for the United States?", and "must we collaborate and confront?"[103].

The report on Chinese military power is an attempt at defining what China is, what it represents, the course it is taking and the consequences of its choices for the rest of the world.

But is this subject seen by the Americans with the objectivity and impartiality required for its analysis? Are there not too many traditions, biases, ulterior motives and predefined objectives in the methodology? The report on Chinese military power could be called "Report on the Chinese threat". The same elements being used from year to year, the lack of updates on the words or data just contribute in rehashing the same simple ideas that will be used in the media all over the world as a source of reference. The views promoted by official reports and the media coverage transform the "Chinese threat" into social reality[104]. The report does not identify a Chinese threat; it is a fabrication of the threat. This Chinese threat connects with the image of a more conventional enemy. Whereas the last decade completely focused on terrorism, an elusive threat, the Chinese threat offers an identified enemy that could be fought with controlled weapons. With the Chinese threat, we also connect with the figure of the spying enemy, whereas terrorism offered only a killer enemy. But the Chinese threat is no longer the same as the old Soviet threat, because between the two there has been the fight against terrorism and the revolution of information technologies. Terrorism changed the feeling

103 See, for example, Eland I., "Is Chinese Military Modernization a Threat to the United States?" *Policy Analysis*, no. 465, pp. 1–14, 2003.

104 '"The China Threat' in American Self-Imagination: The Discursive Construction of Other as Power Politics". Chengxin Pan. http://www.accessmylibrary.com/coms2/summary_0286-14132948_ITM.

of invincibility that was at the core of American society. US–Chinese relations are brought up in this new context of vulnerability. We all know that threats are no longer only nuclear and that a country can be affected remotely, notably through cyber attacks. A "threat" exploits a "vulnerability". If there is a feeling of threat, it is because there is a feeling of vulnerability, of weakness. Doesn't the "Chinese threat" feed a new form of paranoia in American society?

2.4.1.4.11. What do the Chinese think of the report?

The Chinese reacted to the publication of the report quickly. As soon as it was published, comments have been feeding China's Internet sites and traditional media. Here are the most frequently written comments in media articles[105] and from Chinese officials on 4 March 2008[106]:

– the sources of information for this report are questionable. It would seem that complete sections were developed from information taken from the Internet, with no validation of sources and accuracy of content. The information proposed by the report is therefore not reliable;

– the report perpetuates the cold war mentality. This report is the only one published by the Department of Defense involving a particular country, China. During the cold war, the United States published an annual report on the Soviet Union. When the cold war situation relaxed in 1991, the Americans stopped their annual publication. Less than ten years later in 2000, their attention switched to China. For the Chinese, this focus is unacceptable and is revealing of the American mentality of naming an enemy to justify its military budget, its presence and actions all over the world. The attitude of the United States represents a serious violation of international relations standards;

– the partisan presentation of the China–Taiwan relationship, pro-Taiwanese, making the island a weaker player, is in fact an excuse to

105 Google search from the following keywords: 由国防部中国军力报告 2008年.
106 http://news.xinhuanet.com/mil/2008-03/07/content_7736310.htm "The Pentagon report perpetuates the cold war mentality", 7 March 2008. "The spokesman for the Chinese Defense minister categorically opposes the contents of the American report", available at: http://www.pladaily.com.cn/site1/xwpdxw/2008-03/14/content_1163772.htm, 14 March 2008.

reinforce American presence in the Pacific and intensify weapon sales to Taiwan;

– the report distorts truths, false ideas are in abundance because of the very strong subjectivity of the authors of the report, because of bias, preconceived ideas and the ideology that the methodology implies;

– the Chinese are shocked by the accusations made against them in the report: accusations against the Chinese government which allegedly manipulates public opinion, attempting to deteriorate relations between China and foreign countries, an attitude that would be at the source of tensions in the region, etc;

– Chinese culture is peaceful. Historically the country has always been peaceful and will continue to be that way. In 1974, Deng Xiaoping claimed that China would never strive to become a predominant power; the American report prefers to only retain his "24-character strategy", more useful to demonstrate the hidden character of the Chinese threat ("hide our capacities and wait for the right moment"). In fact, isn't the vision of the American analysis warped because the writers cannot discern or find the arguments, able to demonstrate that China is a potential threat, that they are looking for?;

– the report continues to spread a false and ridiculous "theory of the Chinese threat" and the tone of the report has not changed since the first document was published in 2002. It spreads a false truth on the state of Chinese military power. On the other hand, the development of appropriate military capabilities is a legitimate right for any sovereign government. It is also legitimate that China has an army in relation to the status that its new economic power gives it; both forms of power mutually support each other. Finally, because of its military capacities, China participates in maintaining peace in the world. Since 1990, it has participated in United Nations peace operations in Cambodia, Congo, Liberia, Sudan and Lebanon;

– "China's opacity" is "nonsense", is another comment. How can we speak of opacity with military choices when we know that the country has carried out 18 joint military drills with international forces since 2002? On the contrary, transparency has increased and this

should be written in the report because China now submits to the system of military transparency of the United Nations.

2.4.1.4.12. Annual reports from the American Department of Defense on the Soviet Union: From the Soviet Union to China

The series of reports on Chinese military power is the equivalent of the long series of reports on "The Soviet Military Power" published from 1981 to 1991[107]. The first publication of this report on the Soviet Union was a secret modified version, initially addressed to NATO authorities and written by the intelligence agency of the American Defense Department. The report addressed the inventory of Soviet military capacities, "the devil's empire" whose intentions represented a threat to the world. The content of the report justified the fact that NATO countries invested in their military. But, subsequently, reports made public could only demonstrate the problems that American intelligence departments had in understanding the actual situation in the Soviet empire, and did not lead to any new information on the position and role of the Soviet Union. The United States stopped publishing reports on Russia. A few years later, in 2000, it started looking at China, the idea being probably that one day the United States would once again confront an enemy and that this role would be played by China and not India, Russia or Europe. Multiple observers in the world denounced the content of this report which at most draws, and at worst manufactures, the image of the next biggest enemy to the United States, and thus to the world. The accusations made against China are often identical to the ones that were made in the publications on the Soviet Union: lack of transparency, army modernization, race to weaponry, massive investments in defense, etc. And, as with the Soviet Union, the report on China is the only report from the DoD that has been made public.

2.4.1.4.13. Identification of similarities between Russian and Chinese strategies

Is it possible to identify similarities between Russian and Chinese strategies? The report on the Soviet Union from 1981 described the Soviet concept "as an infrastructure of influence", that would consist in the mix and intervention of war forces including unconventional,

107 http://www.fas.org/irp/dia/product/smp_index.htm.

diplomatic, traditional intergovernmental, military council, treatises, agreements and support for terrorist organizations and pro-Soviet guerrilla groups, economic support, cultural support, media, and the use of active measures such as propaganda. This "infrastructure of influence" thus grouped the series of methods of space penetration that remained inaccessible to Soviet military forces[108]. The report on Chinese military power again uses this approach to an extent by recalling the existence of the Chinese concept of the "three wars", approved by the Central Committee of the Communist Party in 2003, that would define the non-kinetic way to conduct modern warfare: psychological warfare (use of propaganda, deception, threat and pressure to affect the capacity of understanding and decision of the enemy), media war (dissemination of information to influence public opinion and obtain the support of national and international opinion for Chinese military interventions), legal war (using national and international laws to ensure the support of the international community and manage the possible repercussions of Chinese military actions)[109].

The object of this 2008 report from the American Department of Defense is to attempt to respond to the question "must we fear China?", or more precisely perhaps, "must the United States fear China?". There are still many uncertainties, grey areas and misunderstandings. Because China does not communicate information in the standard format desired by American observers, because Westerners may not always understand all the intricacies of the language, whatever the reasons, the United States interpret these grey areas and zones of silence as deliberate, so that China can hide its cards. Even while the United States congratulates itself on China's accession to the role of new peaceful economic player, it does not miss an opportunity to depict China as a threat, wrapped up once more in its role as "hero" ready to defend humanity against the "big bad wolf".

---

108 Edgar Ulsamer, *Soviet Military Power*, December 1981, available at: http://www.afa.org/magazine/dec1981/ 1281sovietpower.asp.

109 Page 19 of the 2008 report.

While Western countries denounce China's actions in cyberspace, potentially providing arguments in favor of the American position, agreeing with its predictions and observations, paradoxically the 2008 Department of Defense Report only gives the "information warfare" chapter a relative, perhaps even minimal, significance. In this period of so-called major risks of attacks against sensitive State information systems and attacks in the information field, very little is written in the report about information warfare, especially nothing new or very concrete. This may mean that the United States does not think the cyberspace threat is major, but simply an element among others constituting the Chinese threat.

2.4.1.5. *2010–2015 DoD reports concerning Chinese military power*

The 2010 report from the Department of Defense on the development of Chinese military power[110] still mentions multiple times of the concept of "information warfare":

– "In 2009, the PLA focused training and exercises on command and control, joint ground and air coordination, mobility and mobilization in information warfare, and assault operations";

– "In 2003, the CCP Central Committee and the CMC approved the concept of "Three Warfares" (san zhong zhanfa (三种战法)), a PLA information warfare concept aimed at influencing the psychological dimensions of military activity";

– "China is pursuing a variety of air, sea, undersea, space and counterspace, and information warfare systems";

– "China is improving information and operational security to protect its own information structures, and is also developing electronic and information warfare capabilities, including denial and deception, to defeat those of its adversaries. China's 'information blockade' likely envisions employment of military and non-military

110 Department of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2010, Office of the Secretary of Defense, Washington D.C., 2010, available at: http://www.defense.gov/Portals/1/Documents/pubs/2010_CMPR_Final.pdf.

instruments of state power across the battlespace, including in cyberspace and outer space. China's investments in advanced electronic warfare systems, counter-space weapons, and computer network operations–combined with more traditional forms of control historically associated with the PLA and CCP systems, such as propaganda and denial through opacity, reflect the emphasis and priority China's leaders place on building capability for information advantage".

In this report, a paragraph is devoted to this concept, which the report attempts to define by reference to a number of Chinese publications: "A November 2006 Liberation Army Daily commentary outlines: [The] mechanism to get the upper hand of the enemy in a war under conditions of informatization finds prominent expression in whether or not we are capable of using various means to obtain information and of ensuring the effective circulation of information; whether or not we are capable of making full use of the permeability, sharable property, and connection of information to realize the organic merging of materials, energy, and information to form a combined fighting strength; [and] whether or not we are capable of applying effective means to weaken the enemy side's information superiority and lower the operational efficiency of enemy information equipment.

Thus, this Chinese information warfare would simultaneously mobilize:

– action on information;

– electronic warfare;

– "cyber" operations (the expression used then being CNO);

– civilian and military actors;

– units integrating electronic warfare and CNO.

The 2011 report[111], for its part, devotes more space to the topic of cyber warfare and specifically the capabilities China has developed in

111 Department of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2011, Office of the Secretary

this area. In this section, the authors stress the intrusions to which the American government's networks have fallen prey over the past year – attacks which have been traced to China. China, for its part, mentions the capabilities of cyber warfare which the other great nations are developing. The discourse of each of the countries echoes that of the others. Whilst China stresses the need to ensure cybersecurity, the United States believe that these defense capabilities, which they accept are legitimate, can also be used in military operations (and thus implicitly for aggressive purposes) – particularly, served by:

– data collection (intruding into systems and extracting data);

– limiting an adversary's freedom to act by interfering with their connected logistical bases and communications;

– and serving to multiply strength, when they support or complement kinetic attacks during periods of crisis or conflict.

This report draws a clear distinction between cyberoperations and information warfare, and notes that whilst China has formulated its strategy of deployment of information warfare capabilities in documents which are now considered authoritative (Science of Strategy, and Science of Campaigns), these documents also deal, in parallel, with cyber warfare capabilities. The United States observe and interpret China's military developments as instruments of an anti-access/area denial (A2AD) strategy, which consists of deploying resources to deter or counter any adversary on land, at sea, beneath the waves, in space, in the information domain. The information warfare systems and the operational concepts associated with them serve this A2AD strategy.

In 2013, the report[112] concentrates its discourse on the "information" and "cyber" aspects of two sections: "military information operations" and "cyber warfare in China's military".

---

of Defense, Washington D.C., 2011, available at: http://www.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf.

112 Department of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2013, Office of the Secretary of Defense, Washington D.C., 2013, available at: http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf.

Thus, it is no longer a question of "information warfare". The Americans use their own concepts to describe the strategy and the various operational levels in these two spaces. According to the United States' interpretation, in regard to Chinese publications and declarations, information operations are:

– primarily composed of defensive operations;

– a non-conventional weapon of war;

– a pre-emptive strike weapon (to achieve the state of information dominance and control the electromagnetic spectrum);

– a tool which would enable China to win an information campaign, preventing the need to resort to conventional military action;

– multiple, because they must be designed and adapted for various contexts ("island-landing campaign IO, blockade campaign IO, fire power attack campaign IO, border counterattack campaign IO, counterlanding campaign IO, and counter-airstrike campaign IO") and notably subject to the constraints specific to each domain (land, air, sea).

The United States view the multiple exercises organized by the Chinese army as a demonstration of its capabilities in the field of information.

Cyber warfare, for its part, fits into military operations on three levels: by facilitating the collection of intelligence data, to limit the adversary's action and finally as a strength booster. Thus, here we see the same formulations as in the 2012 report.

The 2014 report[113] makes little change to the discourse developed over the previous years. It recaps the importance of space and of operations in that milieu, in informationization, for informational dominance. What we can take from this report are the sections dealing

113 Department of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2014, Office of the Secretary of Defense, Washington D.C., 2014, available at: http://www.defense.gov/Portals/1/Documents/pubs/2014_DoD_China_Report.pdf.

with operations in space (counterspace), informationized warfare and cyberspace. Information warfare (or informationized warfare) depends heavily on the capacity to use systems deployed in space (and prevent adversaries from accessing these systems). China does not formulate any doctrine specific to operations in space, but they are an essential component of defense strategy centered on the process of informationization. There can be no informationized warfare without control, mastery, security of space systems, without specific operations. Satellites are the central pieces in this architecture, and constitute prime targets.

On the issue of cyber operations, the United States once again highlights the attacks to which they have been subject, attributable to the Chinese authorities, and then repeat the main crux of the arguments and descriptive elements formulated the previous year.

The 2015 report[114] again distinguishes between information operations and cyber operations, and again draws on the concept of "information warfare", here reduced to the rank of "capabilities", which feed into information operations. The overall objective of information operations is the control of information: "information blockade", "information dominance", "information advantage". In order to achieve this objective, it is necessary to combine the operations of information warfare and electronic warfare, acting both in cyberspace and in space. Superiority in cyberspace, therefore, is an instrument to serve this general objective. The report continues with the denunciation of the Chinese cyber attacks Chinese against the United States.

2.4.2. *Evolution of analyses and discourse about Chinese strategy*

The majority of the information available to us about China's practices, policies and strategies in terms of cybersecurity and defense

114 Department of Defense, Annual Report to Congress. Military and Security Developments Involving the People's Republic of China 2015, Office of the Secretary of Defense, April 7, 2015, Washington, available at: http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.

is rooted in English-speaking discourse, dominated by the American perspective, as America is a major producer of reports, studies and discourse on the subject. Cybersecurity companies (Mandiant, Novetta Solutions, etc.), the media, the chiefs or ex-chiefs of government agencies, but also the world of academic research and think tanks have all been discussing the question since the start of the 2000s[115]. China has also been communicating – through the media, official publications and speeches – about its vision of cybersecurity and its analysis of the challenges posed by cyberspace for society and security. On these bases, let us attempt to identify the main evolutions of Chinese cybersecurity/cyberdefense over the past few decades, or at least of Western impressions of them.

The recent cyberstrategy published by the US Department of Defense (April 2015)[116] views China as a centerpiece, if not indeed the centerpiece, in the environment of the cyberthreat. This consideration has not been modified at all over the years, with China always constituting a threat because of its increasing capability and its strategic maneuverings in cyberspace, which are confirmed by a demonstration of sustained effectiveness, looking at the multiple cyber attacks attributed to the country since the 1990s.

The way in which Chinese hackers are described in 2015 differs from the description of them in the 1990s–2000s. Then, more emphasis was placed on "patriotic", "nationalist" hackers – "hacktivists" – who, motivated by patriotic sentiments, acted either on the initiative of, or in concert with, State actors. Frequent mention was made of these hackers' operations (mass Website defacements, intrusions into State servers) which fitted into the contexts of Sino-Japanese or Sino-American crises. Now, the designated hackers are primarily those employed by the Chinese military intelligence

115 An overview of the sources and various approaches proposed by each of them is given in: Daniel Ventre, "Discourse Regarding China: Cyberspace and Cybersecurity", in *Chinese Cybersecurity and Defense*, ISTE-Wiley, July 2014.

116 U.S. Department of Defense, The DoD Cyber Strategy, 2015, Washington, available at: http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

services. Beijing is constantly being accused of involvement in worldwide network disturbances. However, the fact of attention having moved toward State practices does not mean that communities of civilian hackers or cybercriminals no longer exist or are less active than before.

The United States seems to have found the frame of reference which it lacked in the 2000s. Having, up until then, criticized China's cyberdefense strategies for their lack of transparency, and hesitated between describing Chinese cyber-power as presenting a threat of war/conquest, an economic threat or cybercriminal threat, today the United States tends to point the finger at the "economic threat" constituted by the cyber espionage practices employed by the Chinese army. The American authorities essentially view China as stealing intellectual property: thefts committed by the Chinese military intelligence for the benefit of their civilian and military industries, and of course to the detriment of any American competitive edge. Hence, cyber espionage stems essentially from economic warfare.

The threats of regional inter-State conflicts involving China, which will now always include a cybernetic dimension, have by no means subsided. Although the threat of an attack on Taiwan, mobilizing a strategy of information warfare and cyberdefense, has not disappeared, the issue does appear to be less prominent in American strategic analyses. This threat is no longer so systematically mentioned as it was in the 2000s. Other crises do still endure, though: this is attested by the recent territorial tensions between China and Japan or between China and India.

The United States, but also all the countries who claim to have been the victims of Chinese aggressive practices (intrusions into industrial and State systems – APT[117]), have difficulty in conducting a constructive dialog with China, in finding genuine dissuasive measures. The prosecutions, which begun in May 2014 against a number of Chinese army officers accused of economic cyber espionage, are not likely to alter the determination of the aggressors and serve as a dissuasive threat. China, in the face of the repeated

117 APT = Advanced Persistent Threat.

accusations, maintains its position, systematically denying its involvement.

Internally, but with strong international connections, note that the efforts by the Beijing authorities to dominate the information space have not helped reduce violence and protests (Xinjiang, Tibet) in the slightest. The operations in information space, the measures taken in cyberspace (influence, control, surveillance, censure, application-blocking, severance of communications, etc.) have not helped to pacify the regions affected by these crises.

Cybersecurity is indubitably one of the major issues in Chinese society today. However, the country also faces other enormous security challenges, which are just as pressing, if not of even higher priority. The conditions of economic development, of the frantic race for profit, for growth, for enrichment, have had major consequences for society: environmental pollution, climate, health and safety, are vital priorities. The society of the Internet, and of new information technologies, has contributed to the destruction of the environment. China is amongst the nations worst affected by the phenomenon.

On the industrial level, China has acquired skills which it did not possess in the 1990s. It is no longer content with acquiring foreign technologies, as might have been the case; it is not content with being the world's manufacturer: it has become a creative force, improved its process of R&D, created industrial clusters throughout the country, and is able to export its technologies, to gain significant market shares, and to buy foreign businesses. China is attempting to impose its own solutions. Undoubtedly to block its path (for obvious reasons of the struggle for market share, just as much as to deal with true national security issues), a number of States have opposed Chinese companies' access to their national markets. Faced with the threat of economic conquest by Chinese, States are putting up barriers justified by national security, and the need for "sovereign" technologies. For its part, China too is imposing strict constraints on foreign businesses present in its territory (such as the obligation to use security systems (cryptography systems) approved by Beijing, the prohibition of Chinese banks from adopting non-Chinese systems and

applications)[118]. Thus, in numerous countries, Huawei has found itself at the gates of state markets in segments defined as sensitive/vital. The Chinese market itself has been transformed considerably: China's version of Web 2.0 now has its own national industries, with leaders such as Baidu (search engine) and Weibo (the Chinese equivalent of Twitter). China has become a global actor, in the sense that it now has industrial capabilities to cover all three layers of cyberspace (layer 1: creating infrastructures, developing hardware, and industrializing its production; layer 2: creating, developing and commercially imposing software applications, including in Web 2.0; layer 3: creating and developing social network platforms, creating content, and raising awareness of that information layer), and that this mastery extends far beyond its own national borders, conquering shares of markets which have hitherto been dominated by Western or Japanese companies. This industrial strength and the prospects opened up by R&D, supported by political planning, open up prospects for future developments: the Internet of Things, smart cities, big data, but also strengthening of the national and sovereign nature of the solutions adopted in the Chinese sphere. All of this lends China real power and an ability to influence the configuration of cyberspace even today, and even more so in coming years. This power contributes to the evolution of the ratios of strength on the international stage and to China's capacity for influence.

China has attempted to exploit the context of international tension in the wake of Edward Snowden's revelations on surveillance practices, to influence international perceptions of it. Snowden's revelations aroused indignation, questions about the practices of democratic states (surveillance), and about the direction of the relations of trust between states. The criticisms traditionally leveled at China have been turned around against the "model" which America wanted to present: responsible for cyber attacks, intrusions into State servers of foreign powers – even its allies – data theft, political and economic espionage, and surveillance of citizens. This similarity between the practices of states (even though the United States legitimize their practices by citing motives that are different to those

118 "US voices concern over China's banking technology restrictions", *RT.com*, 27 March 2015, available at: http://rt.com/business/244589-usa-china-wto-cybersecurity/.

of China) may contribute to relativizing the nature of the Chinese "threat". The Beijing authorities, in any case, have played on this situation to defend themselves against the accusations leveled at them by Washington and a number of other powers. The day after the accusations of cyber espionage against its military officers, Beijing accused Washington of hypocrisy, recalling that the United States are in control of most technologies and possess the key infrastructures to conduct mass cyber surveillance (espionage) operations, on a global scale, targeting governments, businesses and populations[119].

Cyberspace issues have become the subject of official debates at the highest level between China and numerous other countries: thus, the American and Chinese authorities conduct a bilateral discussion about cyberspace (Sino–U.S. Cybersecurity Dialogue[120], Cyber Working Group), about the need to define rules for security in cyberspace (e.g. aimed at preventing any risk of interpretation, which could lead to an escalation of violence between the states). These exchanges have been suspended due to the quality of the diplomatic relations: dialog in the Cyber Working Group was suspended by China in May 2014. China more generally wants to make itself heard internationally, and claims to be open to bilateral dialogs[121] on the issues of standardization and governance of cyberspace, one of its *leitmotivs* being the defense of sovereignty. Therefore, China has a presence in the standardizing bodies (e.g. the ITU), and is formalizing agreements with foreign partners (for example, in May 2015, the Chinese signed an agreement with Russia, which the media have dubbed the "Cyber Pact"[122]).

---

119 Ben Knight, "US goes after China over cyber attacks", Deutsche Welle, 20 May 2014, available at: http://www.dw.de/us-goes-after-china-over-cyber-attacks/a-17648859.

120 Bilateral Discussions on Cooperation in Cybersecurity China Institute of Contemporary International Relations (CICIR) – Center for Strategic and International Studies (CSIS), June 2012, available at: http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf.

121 "China to deepen int'l cooperation on cyber security", *CCTV.com*, 10 February 2015, available at: http://english.cntv.cn/2015/02/10/VIDE1423536244824155.shtml.

122 Alexandra Kulikova, "China–Russia cyber-security pact: should the U.S. be concerned?, Russia Direct, 21 May 2015, available at: http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned. An

Thus, today, China is one of the major actors on the international scene in terms of exploitation of cyberspace for political, strategic and military ends. However, it is still lagging behind the American superpower. In addition, the world context has also changed greatly since the 1990s: since 2007, but particularly 2010, ever-increasing numbers of states have committed to a process of development of policies of cybersecurity and cyberdefense, in the implementation of civilian and military capabilities, to secure and protect their assets, their systems, but also envisage the use of more "aggressive" practices in cyberspace, even in peace time. China itself has admitted the existence of its dedicated cyberdefense units (this acknowledgement was included in the latest version of The Science of Military Strategy, published in 2013)[123]. Thus, it is the world context which has undergone major evolutions in terms of cybersecurity in recent years. We can envisage a number of consequences, for China, of these new equilibria, new policies, institutions and practices:

– toughening of targets, theoretically rendering the task more difficult for attackers, Chinese or otherwise, and forcing them to improve their offensive know-how;

– the increasing power of aggressive capabilities in numerous countries opens China up to more numerous attacks – at least theoretically;

– the power acquired by China also leaves it exposed to more numerous cyber attacks;

– China's increased dependence on cyberspace, with ever-increasing numbers of components of its society connected to public networks, exposes it to aggressive actions by foreign powers, and more generally by hackers of all backgrounds, with a wide variety of motives.

English translation of the agreement is given at: http://www.csistech.org/blog/2015/5/11/sino-russian-cybersecurity-agreement-2015.

123 Shane Harris, "China reveals its cyberwar secrets", *The Daily Beast*, 18 March 2015, available at: http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html

With 632 million Internet users and 242 million e-commerce users, China is a prime target for hackers
45.7% of mobile terminals were pirated between November 2013 and October 2014
At the end of 2012, nearly a third of the 200 million Chinese online buyers had fallen prey to deception or fraudulent transactions on online sales sites
According to the Norton Report 2013, China is the second country in the world most affected by cyber crime

Table 2.3. *China as a target for cyberthreats*

Strategy	
	Reinforcing China's power in the world
	Countering hegemonic power
	China is more than an alternative, a counterweight to the hegemon. A world centered on Asia; on China
	Ensuring the CPC remains in power and its ideology remains prevalent
How China views the strategic role of cyberspace	
	Cyberspace is merely one area of expression of power, among others
	Cybersecurity is simply a subset of national-security issues
	The cyberstrategy of defense is consistent with the defense strategy of which it is part: active defense
	Occupying all domains (land, air, sea, space and cyberspace)
	Being capable of projecting its power as far as possible in all environments
	Claiming sovereignty in cyberspace

Cybersecurity: *Focus on layer 3*	
	Cybersecurity/defense is exercised in response to an external threat – mainly Western: espionage, and ideological destabilization
	Since the start of the 1990s: Centered on "information warfare" in its military and civilian dimensions
	It is important to protect China from the risks of ideological destabilization: influence, propaganda
Strategy: Building Chinese power, constructing the image of power. *Methods:*	
	Bilateral versus multilateral in the area of cybersecurity (Sino–Russian agreement)
	"Dialogs" with the West
	Presence in international organizations
	Offering a model of cybersecurity
	Contradicting, refuting
	Affirming its pacific intentions
	Playing the role of victim (legitimizing the posture of active defense)
	Increasing the number of domains of power: economy, culture, security, defense and cyber
	Policy for a digital society (example: Internet Plus project)
	Industrial policy on NICT: with its incubators, industrial zones, innovation support programs, military-civilian cooperation, projects (Internet of Things, smart cities, robotics, etc.)
	Technological autonomy: China has its own operating systems, its own Web 2.0, etc.
	Building capabilities of military cyberdefense, for local wars
	Legitimizing increased militarization: for a great power, imposing defense forces are needed

Table 2.4. *Overview: China's strategies, the role of cyberspace and information*

2.4.3. *China as a "victim"*

In international relations, victimization (or "victimhood") through discourse (a process which entails presenting oneself as a victim of others) has been identified in many contexts (e.g. the tensions between Vietnam and China[124]).

Claiming victim status is an act which legitimizes, explains and justifies choices and acts, which are therefore qualified as legitimate and fair reactions. The discourse may be rooted in the immediacy of the threat faced, and be produced when the target is reacting; when we are calling on others to come to our defense, when we wish to raise awareness to spur action (in which case, on the one hand, we can appear to be a victim, but on the other, we appear dependent and submissive – at any case, dependent on the power of a third party, whose intentions, alliance and trust we are testing, on which future relations will depend); but that discourse can also be sustained over the fullness of time, in political speeches, in history books (which are notably at the heart of the tensions between China and Japan, with both accusing the other of rewriting history to its own advantage[125] and presenting itself as a victim).

This victimhood is often accompanied by a discourse of demonization of the enemy, which renders the status of victim all the more convincing. This strategy can be employed, for example, to mobilize a national community, to obtain international support, or to trigger reactions.

It is also these objectives which states pursue in painting themselves as victims of cyber attacks. There is also a sort of one-upmanship in the discourse, with the United States and China each claiming to be the main victim, saying that they have suffered the

124 Huong Le Thu, "The role of victimisation in the Vietnam-China War of Words", *E-International Relations*, 5 July 2014, available at: http://www.e-ir.info/2014/07/05/the-role-of-victimisation-in-the-vietnam-china-war-of-words/.

125 Alexander Bukh, "Japan's History Textbooks Debate: National Identity in Narratives of Victimhood and Victimization", *Asian Survey*, University of California Press, vol. 47, no. 5, pp. 683–704, 2007.

greatest number of attacks. Thus, each state feels it is more of a victim than the others.

This discourse generally points the finger at other states, and less frequently at private actors or individuals. The targets threatened by the attacks are a state's sovereignty, peace, social equilibrium, and the nation threatened with influence.

Discourse is designed to convince the audience of the well-foundedness of defense policies, strategic choices, and also helps to fortify alliances and convergences (cybersecurity agreements between two or more states).

America, when affected by cyber attacks, revealed its defensive strategy: active defense, pre-emptive and preventative operations, counter-attack, diplomatic measures (dialog) and judicial pursuit (accusation of Chinese officers: in reality, this is a judicial counter-attack which is targeted at individuals rather than a state – at least, directly). America is a determined victim, prepared to make use of all resources and all possible measures to defend itself.

China does the same, as indeed do many other countries the world over. There is a kind of struggle, a battle to hold the title of victim, because it shifts the blame for guilty behavior onto the other party.

2.4.4. *The strategy of active defense*

The concept of active defense was introduced in 1955 by Minister of Defense Peng Dehuai and Mao Zedong to describe Chinese military doctrine[126]. That military doctrine was publicly announced on 6 March 1957 by Peng Dehuai in a report ("On the Direction of the Fatherland's Military Doctrine and National Defense Construction") to the Central Military Commission: coordination of political, diplomatic and military resources; "no first strike" strategy; readiness

126 Yuan Dejin, Wang Jianfei, "The historical evolution in the direction of military doctrine since the founding of New China, and the lessons from it", June 2007, available at: http://www3.nd.edu/~pmoody/Text%20Pages%20-%20Peter%20Moody%20Webpage/Military%20Doctrine.htm.

to counterattack when faced with imperialist aggression (from the United States), stabilizing the front line, waging a "protracted" war, depriving the enemy of the initiative of attack; moving from a defensive posture to an attacking posture. Even as early as the 1950s, this doctrine portrays the United States as the imperialist enemy. In 1977, the strategy became one encouraging enemies to penetrate deep within the lines (i.e. strategy which involves allowing the enemy to infiltrate deep within the territory, and then catch them). This strategy holds that it is not necessary to defend all positions; losing some such positions, temporarily, can actually prove beneficial, in that it allows China to entice and then ensnare the enemy. In the 1980s, China returned to a doctrine of active defense, leaving aside that of "tempting the enemy in deep". In 1985, Deng Xiaoping wrote that active defense involves strengthening the deterrent, promoting peace, and remaining prepared for small-scale local wars, but also fighting to forge an international environment which is more favorable to China. The strategy of *tempting the enemy in deep* was abandoned, and replaced by the defense of key points from the very earliest days of a war. Active defense is not just defense, pure and simple. It contains the strategy of "protracted war". This was the doctrinal context into which the concept of high-tech localized wars (Fighting and Winning a Local War Under high tech conditions), in the late 1980s to early 1990s. The doctrine focuses on local wars rather than widespread international wars.

Active defense applies to all China's defensive forces; its implication is that China will only launch a military strike after having been struck itself (by an adversary who may not necessarily be military). The first blow may also be not military but political and strategic, but inviting a military response (which, from a tactical standpoint, is not then considered as being the first strike). Thus, this active defense can only realistically be envisaged by maintaining an offensive operational stance[127].

127 Anthony H. Cordesman, Ashley Hess, and Nicholas S. Yarosh, Chinese Military Modernization and Force Development A Western Perspective, CSIS, Washington, p. 73, 23 August 2013, available at: http://csis.org/files/publication/130725_chinesemilmodern.pdf.

America's intrusive cyber operations, and the political and diplomatic attacks (accusations) made against China, could therefore be considered by China to be acts of aggressions, warranting a reaction. When transposed to cyberspace, active defense is connected to the idea of counter-attacks ("hack-backs") targeting the attacking hackers. Active defense is based on 5 principles: vigilance, detection, attribution, prevention (i.e. what can be done to prevent the attacks), and retribution[128].

128 http://www.welivesecurity.com/2013/11/19/active-defense-good-protection-doesnt-need-to-be-offensive/.

3

Russia

There are many observers who view Russia's practices, both within its borders and beyond them in its conflictual relations on the international scene, as revealing a specific information-warfare strategy. This would be one of the defining features of the security and defense policy, and of the Kremlin's strategy for exercising power. The West appears to have lost interest, somewhat, in Russia's ambitions in the domain of information warfare[1]. This lack of familiarity partly accounts for the effect of surprise[2] produced by the Russian information operations carried out in Georgia and then in Ukraine. These capabilities and information-warfare operations are qualified as aggressive[3], targeting a Western

1 "I've worked closely with a recently retired Russia analyst from the IC for the past six years and he has confirmed to me that since the end of the Cold War, Russia has never been a high priority for U.S. policymakers. Indeed, no one has wanted to be bothered by potentially problematic briefings about Russia." Jeffrey Carr, Russian Cyber Warfare Capabilities in 2014 (We aren't in Georgia anymore), Digital Dao, March 8, 2014, http://jeffreycarr.blogspot.fr/2014/03/russian-cyber-warfare-capabilities-in.html.

2 Edward Lucas, "Russia's Information Warfare, European Voice", Politico.eu, November 2014, http://www.politico.eu/article/russias-information-warfare/.

3 Bill Gertz, "House adds funds to counter Russian info war", *Washington Times*, 29 April 2015: http://www.washingtontimes.com/news/2015/apr/29/inside-the-ring-house-funding-bill-targets-russian/?page=all.

Information Warfare, First Edition. Daniel Ventre.
© ISTE Ltd 2016. Published by ISTE Ltd and John Wiley & Sons, Inc.

enemy[4] (Russia's information warfare strategies are also being constructed in opposition to Western concepts)[5]; they are at the heart of the power strategies in Crimea[6], in the Baltic nations[7]. Russian information warfare is again the subject of theoretical analyses[8] and is arousing multiple interpretations (as regards the "weaponization" of information[9]; the central role of information warfare in hybrid wars[10]; the innovative nature of the Russian approach in terms of information warfare[11]; the superiority of Russian capabilities in the

4 Anton Shekhovtsov, "The Challenge of Russia's Anti-Western Information Warfare", Diplomaatia.ee, April 2015: http://www.diplomaatia.ee/en/article/the-challenge-of-russias-anti-western-information-warfare/.
Roger McDermott, "Russia's Information Warfare targets Washington and NATO", *Eurasia Daily Monitor*, vol. 12, Issue 74, April 2015: http://www.jamestown.org/programs/edm/single/?tx_ttnews%5Btt_news%5D=43816&cHash=3a264329f53ee50e0b556cdfa4fefc8c#.VfguvhHtmko.
5 Jolanta Darczewska, "The anatomy of Russian Information Warfare. The Crimean Operation, A Case Study", *Point of View*, Warsaw, no. 42, p. 37, May 2014, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.
6 Jolanta Darczewska, 2014, *idem*.
7 Agnia Grigas, Russia's Information Warfare in the Baltic States, Part I, December 29, 2014, http://en.delfi.lt/lithuania/foreign-affairs/anatomy-of-russias-information-warfare-in-the-baltic-states.d?id=66767990, Part II, December 30, 2014, http://en.delfi.lt/lithuania/foreign-affairs/russias-information-warfare-in-the-baltic-states-ii.d?id=66778660.
8 Timothy L. Thomas, "Russian Information Warfare Theory. The consequences of August 2008", *The Russian Military Today and Tomorrow*, July 2010, http://mercury.ethz.ch/serviceengine/Files/ISN/118969/ichaptersection_singledocument/d550520b-4937-4967-a3f5-38fbc5d76b48/en/Chapter_4.pdf.
9 Helle C. Dale, Russia's "Weaponization" of Information, Testimony Presented to the House Foreign Affairs Committee, April 15, 2015, http://www.heritage.org/research/reports/2015/04/russias-weaponization-of-information.
10 Eve Hunter, Piret Pernik, The Challenges of Hybrid Warfare, International Centre for Defence and Security, Tallinn, Estonia, p. 7, April 2015, http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf.
11 Peter Pomerantsev, How Russia is Revolutionizing Information Warfare, September 9, 2014, http://www.defenseone.com/threats/2014/09/how-russia-revolutionizing-information-warfare/93635/.

domain[12]). In this chapter, we examine the different explanatory theories and hypotheses and discuss them: it is useful to examine whether information warfare at the time of writing in 2015 actually reflects the same reality as in the 1990s-2000s, and to discuss the supposed "renewal" of information warfare in light of Russian doctrine.

Idea	Comment
Information warfare consists of waging war through non-military means[13].	This idea is not, strictly speaking, particular to discourse on modern Russian information warfare. The idea was already there, underlying the definitions of information warfare in the 1990s-2000s, and indeed was one of its fundamental elements.
Information is used as a weapon.	This consideration is not specific to Russia.
Information warfare characterizes hybrid wars, which are exemplified by Russia's actions in Ukraine since 2014[14]. The essential element of the information warfare which characterizes this hybrid war is reflexive control, which leads the adversary to make decisions and adopt stances which run counter to his own interests[15].	This is one of the fundamental principles of information warfare. There is no innovative nature here.

12 James C. Coyle, Russia has complete information dominance in Ukraine, May 12, 2015, http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-has-complete-informational-dominance-in-ukraine.

13 Ulirk Franke, "War by non-military means. Understanding Russian Information Warfare", *FOI*, p. 63, March 2015, http://www.foi.se/Global/Press%20och%20nyheter/War%20by%20non-military%20means.pdf.

14 Michael Kofman, Matthew Rojansky, A closer look at Russia's "Hybrid War", Wilson Center, Kennan Institute, Kennan Cable, no.7, p. 8, April 2015, https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.

15 Maria Snegovaya, Putin's Information Warfare in Russia. Soviet origins of Russia's Hybrid Warfare, Russia Report 1, Institute for the Study of War, Washington DC., p. 28, September 2015, http://www.understandingwar.org/sites/default/files/Russian%20Report%201%20Putin's%20Information%20Warfare%20in%20Ukraine-%20Soviet%20Origins%20of%20Russias%20Hybrid%20Warfare.pdf.

Russian information warfare is constructed, on the conceptual level, unlike Western approaches.	In all cases, the purpose is to set up a Russian project to oppose Western intentions.
Circulation of information on the Internet constitutes a threat to society and sovereignty. Hence, it is important to control the circulation of information.	This position is shared by numerous countries. Russia is not alone in this analysis. China is often cited as an example of a country adopting a similar approach.
Defense of the sovereignty of the national Internet is a major issue in national security.	The concept of sovereignty (of the Internet, or industries of cyber technologies) has become important in numerous countries, and thus is not a stance specific to Russia

Table 3.1. *Overview of discourse on Russian information warfare (2015)*

Document	Date
Draft Convention on International Information Security	Released 24 September 2011
Conceptual Views on the Activity of the Russian Federation Armed Forces in Information Space	Released 22 December 2011
Information Security Doctrine of the Russian Federation[16]	2000

Table 3.2. *A few Russian reference documents*

3.1. Military doctrines and national security strategies

Over the past 25 years, various official documents have been published to express the evolution of Russian doctrine and defense strategy. In examining these documents, we can observe the evolution

16 Information Security Doctrine of the Russian Federation, 2000, http://www.mid.ru/bdomp/nsosndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

of the place occupied by information, and information technologies, in this military strategy.

In "The Basic Provisions of the Military Doctrine of the Russian Federation" (1993)[17], the Security Council of the Russian Federation validates the principle of acquisition of high-tech communication technologies: "the development and production of highly efficient systems for the command and control of troops and weapons, communications, intelligence, strategic warning, electronic warfare, and precision, mobile, nonnuclear weapons, as well as systems for their information support". However, the concepts of "information warfare" and "cyber" are not explicitly formulated in the document.

In the new military doctrine published in 2000[18], there is no discussion of cyberspace or cyber warfare. Action in the information field appears as one of the multiple techniques that can be employed to ensure national security (alongside political, economic, social, judicial and military measures). The political and military situation is dependent on multiple risks (nuclear, local wars) where the exacerbation of confrontation in the information field occupies an important place. It is also cited in the text on the same level as the threat constituted by the propagation of nuclear weapons or other weapons of mass destruction. The use of information by diverse entities on the international scene represents a risk of destabilization. We see the two categories of information which represent a threat: information-technical and information-psychological. In its initial phase, a regional armed conflict will involve intense armed confrontations, a struggle for supremacy in the information sphere, and a fight to maintain the upper hand in the aerial arena.

17 The Basic Provisions of the Military Doctrine of the Russian Federation, adopted by edict No. 1833 of the president of the Russian Federation, dated 2 November 1993, http://fas.org/nuke/guide/russia/doctrine/russia-mil-doc.html.
18 http://www.armscontrol.org/act/2000_05/dc3ma00?print.

The military doctrine published on 5 February 2010[19] does not mention "cyber". There again, it is recalled that information instruments are used, similarly to political, diplomatic, military, judicial and economic tools, to protect national interests. Attacks on the information infrastructures are part of the threats that are of concern to armies. The intensification of the role of information warfare is also characteristic of contemporary armed conflicts. Information warfare is assigned two specific functions: firstly to achieve political objectives without needing to resort to the use of armed force; and secondly to help the international community provide the appropriate military response. The other characteristics of these conflicts are: the mass use of armaments based on new physical principles; the mobilization of forces are resources operating in the air and in space; the acceleration of the military process and the decision-making process; the effect of surprise created by the suddenness of the new conflicts. In order to prepare forces to cope with these challenges, they need to be equipped accordingly. Therefore, efforts are devoted, amongst other things, to resources for information warfare.

In the 2014 military doctrine[20], the concept of cyber is still not introduced, and that of information is subdivided. This doctrine, according to the text, defines the conditions of mobilization of the army, only after other means – political, diplomatic, judicial, economic, informational… i.e. all non-violent measures – have been exhausted. The threats and risks which weigh upon the army are increasingly focused on the information sphere. These threats lie in the "use of information and communication technologies for the military-political purposes to take actions which run counter to international law, being aimed against sovereignty, political independence, territorial integrity of states and posing threat to the international peace, security, global and regional stability". The exploitation of information by hostile forces, whether domestic or foreign, constitutes a significant threat in the eyes of the authorities:

19 The Military Doctrine of the Russian Federation, Approved by Russian Federation Presidential Edict on 5 February 2010, http://www.sras.org/military_doctrine_russian_federation_2010.

20 The Military Doctrine of the Russian Federation, Approved by the President of the Russian Federation on December 25, 2014, http://www.rusemb.org.uk/press/2029.

"subversive information activities against the population, especially young citizens of the State, aimed at undermining historical, spiritual and patriotic traditions related to the defense of the Motherland". The use of information resources contributes to new conflicts which are characterized by the use of various measures (military, political, economic, mobilization of the populace in protest movements, etc.), so that the enemy experiences pressure from all sides (air, space, outer atmosphere, land, ocean, information sphere). The document maintains the objective of development of military capabilities of information warfare.

The article published in 2012 by four Russian colonels[21] illuminates the conceptual definitions adopted by Russia. In that article, the information environment takes on the definition given by the Shanghai Cooperation Organization. Thus, the information environment is defined as "a domain where information having an effect on individual and public mindsets, information infrastructure, and information itself is conceived, produced, transformed, transmitted, used, and stored"[22].

The Russian Ministry of Defense Website[23], for its part, offers a number of useful definitions. Let us note the concepts in Table 3.3.

According to this document, it is vital for Russia to fight against information warfare attacks, in an international context where information warfare has become increasingly prevalent, whilst committing itself to respect the norms of international law (in particular, to respect the principles of sovereignty of states, and not to use force) and international humanitarian law (limiting the indiscriminate use of information weapons).

---

21 S.I. Bazylev, I.N. Dylevsky, S.A. Komov, A.N. Petrunin, "The Russian Armed Forces in the Information Environment: Principles, Rules, and Confidence-Building Measures", *Military Thought*, pp. 10–15, 2012: http://eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.2_2012.pdf.

22 Reproduced from: Annex 1 to the Agreement between the governments of the Member Countries of the Shanghai Cooperation Organization on Cooperation in international information security, Yekaterinburg, 2008.

23 Russian Federation Armed Forces' Information Space Activities Concept, no date, http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle.

Military conflict in the information space	Conflict in cyberspace may take place between states or within the state. It becomes a conflict in the information sphere as soon as information weapons are used.
Armed forces cyberspace activities	These activities involve the use of military information resources (in the context of defense and security.). This definition does not allude to any mobilization of resources of non-military actors. In this definition, the information resources are those which the army uses in its cyber activities. Information and cyber are linked, here.
Information warfare	Information warfare is a confrontation between states (this definition thus differs from that of military conflict in information space given above, as it excludes internal conflicts). Information warfare is defined as a set of practices and objectives: – inflicting damage on the enemy information systems, on the process and resources, on the critical and non-critical structures; – affecting the enemy's political, economic and social systems; – carrying out operations of mass psychological manipulation of the population to destabilize the state and society.
Information weapons	Information weapons are: information technologies, means and methods used to conduct information warfare. Note here that methods are held to constitute weapons.
Information space	The information space is composed of a set of operations (creation, trans-formation, transmission, usage and storage) performed on information.

Table 3.3. *Main concepts and their definition proposed by the Russian ministry of defense*

On 9 September 2000, the Russian Federation published a doctrine on information security[24] (approved by Vladimir Putin). The concepts of "cyber" and "information environment" are absent from the document. The following main concepts are employed:

– "information space" (not defined);

– "information sphere": defined as "an assemblage of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, and a system governing public relations arising out of these conditions");

– "information security": defined as "the state of the protection of its national interests in the information sphere, as determined by the overall balanced interests at the level of the individual, society and the state");

– "information war" ("creating means for dangerous attack on the information spheres of other countries of the world, disturbing the normal functioning of their information and telecommunication systems, breaching the security of their information resources and gaining unsanctioned access to them");

– "information weapon" (not defined).

A new doctrine was published in May 2015, motivated by the modification of the international context, taking account of the new realities associated with technological developments (at the time of writing, the text of this new doctrine is not available).

3.2. Information warfare in practice

Estonia in 2007; Georgia in 2008; Ukraine in 2013-2015… Russia is involved in information operations which capture the attention of the international community because they tell us as much about

24 Information Security Doctrine of the Russian Federation, September 9, 2000, http://archive.mid.ru//bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b!OpenDocument.

Russia's capabilities in terms of cyberdefense and information warfare as about its intentions (aggressive, expansionist, challenging of the American hegemony, etc.), its strategies, and its position on the international scene. These events also illustrate the ways in which modern wars progress. Kinetic actions are preceded, accompanied and followed by operations in information space (including cyberspace). Information dominance, conflict and information combat do not render kinetic actions obsolete. Rather the two aspects are mutually complementary.

3.2.1. *Cyber attacks against Estonia. Who is the culprit?*

The news early in 2007 was marked by the announcement of a series of attacks against Estonian information systems and presented by the international press as an example of information warfare against Estonia by Russia.

3.2.1.1. *Reconstitution of facts*

We will try to group the most significant elements from information that was published on different online information websites. The following documents were chosen at random, the way an Internet user would search, surfing the net and moving from one site to another:

– an article entitled "Hackers deepen Estonia–Russia rift" from 17 May 2007[25], published on the Aljazeera website;

– an article entitled "The cyber pirates hitting Estonia", published 17 May 2007 on the BBC News website[26];

– an article entitled "Estonia recovers from massive denial-of-service attack", published 17 May 2007 on the InfoWorld website[27];

25 http://english.aljazeera.net/NR/exeres/4434AB7B-00C7-4140-8234-1043635907FC.htm.
26 http://news.bbc.co.uk/2/hi/europe/6665195.stm.
27 http://www.infoworld.com/article/07/05/17/estonia-denial-of-service-attack_1.html.

– an article entitled “Estonia blames hack attacks on Russia”, published on the website http://p2pnet.net/story/12262;

– an article entitled “Cyber Attack Vexes Estonia, Poses Debate”, published 18 May 2007[28];

– an article published 19 May 2005, entitled “Estonia calls for NATO cyber-terrorism strategy”[29].

What image can we construct of the events from these articles?

A statue paying tribute to soldiers from the red army killed in the Second World War against Nazism was taken away from Tallinn, capital of Estonia. Estonians see in the statue the symbol of Soviet occupation. The Russians, and especially the strong Russian community living in Estonia, perceived the statue’s removal as an attack against Russia. The statue’s removal was a pretext for the start of hostilities between the Russian and Estonian communities in Estonia.

Some say that the real reason for the tensions between the two countries was Estonia’s blocking of the building of a pipeline to Germany.

The incident translated into riots on the streets of Tallinn.

Massive attacks were simultaneously launched in cyberspace:

– DDoS attacks were launched against Estonia’s information systems. The targets were the government, banks and private companies’ websites;

– in the first days of the attacks, websites usually receiving 1000 visits per day suddenly received 2000 requests per second. Some sites overloaded within a half hour;

– over a million computers in the world were used to launch the attacks. These were botnets used to launch DDoS attacks. Computers from the United States, Canada, Brazil and Vietnam were used. The

28 http://online.wsj.com/article/SB117944513189906904.html?mod=googlenews_wsj.
29 http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/18/westonia18.xml.

Estonian Information Technology Center, an agency monitoring the government's computer networks, declared that the cyber attacks came from all over the world, including Russia. According to the Estonian Minister of Defense, instructions in Russian on how to attack websites circulated over the Internet;

– the attacks also included site defacements such as redirection of Internet users, Soviet soldier images, speeches from Martin Luther King and a false message from the Estonian Prime Minister apologizing and promising that the statue would be returned to its original place;

– the attacks started on 27 April 2007 and lasted over two weeks, each wave of attack being stronger than the previous one.

In the context of the Estonian riots, observers, public opinion and the Estonian authorities estimate that the attacks were the direct consequence of the deterioration of political relations between the two countries.

Russians were instantly accused, albeit discretely, of being the authors of these attacks against the Estonian government information systems:

– the Estonian Minister of Defense declared "we have identified in the first attacks IP addresses belonging to departments in the Russian government";

– the Estonian government did not prosecute the Russian authorities, but posted a list of IP addresses as the origin of the attacks. Some of these addresses belonged to the Russian government and the Presidential administration. However, there were also many from other countries;

– the attacks were likened to a terrorist act by the Defense Department. Regardless of who the terrorists were, Estonia, as any country who depends on its information systems (e-government, 98% of transactions made over the Internet), took measures. Protection methods were insignificant so the Estonian government decided to block access to the websites that were attacked.

Estonia did not want to consider this massive aggression simply as a wave of cyber crime, for which a legal solution could be found. Because of the scope of the attack and given the country's inability to find solutions alone, and because it considered such a large-scale terrorist attack an act of war, Estonia requested the help of the international community. Aggressions in cyberspace took on a diplomatic dimension. NATO sent an expert to help Estonia face the attacks against its government's websites.

Why did NATO get involved? Because an attack against one of its members is an attack against the organization itself. The situation took an international political turn. The debate changed levels: it was no longer about finding delinquent individuals but about defining the responsibility of a government, triggering a completely new debate on the political situation, diplomatic relations and regional balances involving Cyber attacks. This wave of Cyber attacks must have made governments question their way of viewing these attacks in the context of international law, and consider what the appropriate response should be.

We must also consider that Russia has also often requested the support of the international community in its fight against cyber crime. Rashid Nurgaliyev, the Interior Minister, called for the world to combine forces to fight against criminal groups operating over the Internet during an international conference in Moscow in April 2006. According to the minister, cyber criminals can cause as much damage as weapons of mass destruction.

The question is "can a government be behind the attack?". In more general terms, the question may be "is it possible to prove that a government is the author of a cyber attack against another government?".

In the case of Estonia, finding proof seems difficult. For now, it is one word against another. Estonia implicated the involvement of the Russian government; the Kremlin formally denied the allegation. The argument for the defense is of course the opposite of the argument for the accuser: according to the Russians, the Kremlin's IP addresses had been the victims of IP spoofing.

In order to conduct these attacks, there is no need for government. The anti-Estonian feeling was developed and maintained by government propaganda and was expressed through articles, blogs, forums and the press. Hackers were immersed in this general feeling and acted accordingly. Even if the government was not directly involved, the anti-Estonian hysteria may have encouraged nationalist hackers. On the other hand, launching attacks is simple, but there needs to be some basic expertise. Virus scripts, source codes and ready-made solutions are found over the Internet. Thousands of budding hackers can launch efficient attacks.

Does reading random articles found on the Internet among hundreds of publications on the subject answer the questions "Could a foreign nation be behind the attack? Can Russia be guilty?". The articles, because of their number and repetitive use of identical information, can only highlight the absence of conclusive elements. An infinite combination of the same basic elements, the "ingredients" in the information, however, does contribute to creating an opinion which may be completely false.

What are the common elements, what are the "ingredients" in these articles, what is being said and what is generally ignored? Do we have all the conclusive elements to confirm that it truly is information warfare? What should we conclude from Russia's position?

A few lines from the article "Hackers Deepen Estonia–Russia Rift" from 17 May 2007[30], published on the Aljazeera website, are interesting because in a single sentence it presents the way things generally related to network attacks are reported: "NATO has sent an expert to help Estonia fight attacks on government websites, which the Defense Minister has said the Russian government was possibly involved in":

– a victim was named, Estonia in this case;

30 http://english.aljazeera.net/NR/exeres/4434AB7B-00C7-4140-8234-1043635907FC.htm.

– the act was addressed. Government websites were attacked. The term "attack" was used, implying an aggression on the government instead of simply hacking (cyber delinquency);

– a guilty party was named: the Russian government;

– there is a reference from a relevant source, made in good faith: the Defense Minister;

– but at the same time, there is a large amount of imprecision ("was possibly involved").

There are enough variables here to start a rumor: a victim, the act committed against the victim, a named guilty party and a source that is highly credible. But we also find lack of proof and sources, and yet a level of precision in the narration of the facts (from a technical point of view, what attacks were conducted, how many sites were affected, etc.). In fact, nothing in this article, or in any other, enables us to confirm or deny the involvement of the Russian government.

The articles also imply relations between the different players and events:

– a relation is established *a priori* between Estonia and Russia, because the context (the events) is greatly slanted that way. However, what attests to the Russian involvement with any certainty? Could the attacks not come from another country and still use Russian systems?

– a relation is also established *a priori* between "hackers" and the "Russian government". Could the hackers not have acted on their own, with no official link to the Russian government?

– a relation is established *a priori* between the riots and cyber attacks. There were riots and cyber attacks. What connects the two? Can there not be two simultaneous events without instant connection?

The way in which incidents were reported, written and handled also shows:

– the importance of subjectivity in the definition and especially the qualification of the incidents: do journalists know what they are talking about (what is a DoS attack? what is site defacement?) Do

they have reliable sources? On what basis do they speak of "information warfare", and what are the irrefutable elements of proof needed to accuse Russia instead of another player?

– the importance that the preconceived image of Russia can have on observers, and in general of any other player. Russia is commonly perceived as a country where cyber criminality rules, it is a country attempting to destabilize its close neighbors, a hoodlum state. In parallel to the growth of networks and number of Russian users, the number of cyber crimes keeps increasing. Cyber crime has multiplied from 2001 to 2005. In 2003, The Interior Minister recorded 7,052 cyber crimes committed via the Internet, 13,713 in 2004 including 8,000 that were intrusions in information systems[31], 14,810 in 2005 and approximately 8,400 in the first six months of 2006[32]. This Russian cyber crime is raging all over the world;

– the predominant place of uncertainty, ignorance, conjecture and suppositions. Observers have a hard time trying to reconstitute real facts for lack of time or resources, or because of a lack of technical expertise. The different views probably include truths, lack of understanding, false assertions in good faith and false assertions in bad faith. But this confusion only confirms the extreme difficulty in making a real accusation against a possible attacker. This attacker takes advantage of the vague nature of the attacks, of the possibility of hiding behind a fake identity, or of the impossibility of proving without a doubt the real identity of the perpetrator, to implement his operations. The denial of allegations from the Kremlin is proof of this difficulty.

The question of IP address appropriation is complex in that either Russia was a victim of identity theft and is not responsible, or the addresses from the other systems in the world used in the attacks were appropriated by Russia, in which case, they would mask their identity behind other governments. If the IP address is Russian:

– the attacker could be the Russian government;

31 *Russia: Authorities warn of Cybercrime Epidemic*, http://www.rferl.org/featuresarticle/2006/04/7d821779-4411-43d1-bf7b-d19743879df6.html, 20 April 2006.
32 http://www.crime-research.org/news/02.11.2006/2327/, 2 November 2006.

– the attacker could be a Russian, or a group of Russians, with no link to the government, or maybe even have a link with other governments who would benefit from the accusations made against Russia;

– the addresses could be appropriated and the attackers might not be Russian. Or they could be Russian and have launched attacks by stealing Russian IP addresses.

However, if the IP address is not Russian, that does not mean that the perpetrator of the attack (or the sponsor) is not Russian! An independent Russian attacker could appropriate a foreign IP address, and the same goes for the government.

The events in Estonia raise questions, but the Estonian case is minor in comparison to the scope of the real problem, which is how to protect the global Internet infrastructure from attacks that, as with the viral attack in February 2007, can block a part of the world's Internet.

3.2.1.2. *Doctrines and components of the "information warfare" concept*

Suspicions, allegations and accusations against Russia raise several questions. Is Russia able today to start significant information warfare operations[33]? Is there an official doctrine that includes these operations? Who could implement such operations?

In the 1990s, the Federal Agency for Government Communications and Information (FAPSI) identified five major components:

– electronic warfare;

– intelligence warfare (i.e. search for information from radio signals, satellites and radars through interception and decryption of information flows);

– hacker warfare (cyberwar);

33 In order to better understand the reflection on the impact of the Desert Storm campaign on the Russian doctrine and understanding future wars, please refer to M.C. Fitzgerald, *The New Revolution in Russian Military Affairs*, Royal United Services Institute for Defence Studies, London, 1994.

– psychological warfare;

– collection and processing of open source information.

For the Foreign Intelligence Service (SVR), information warfare is achieving superiority of information by controlling the information resources of other governments (i.e. by banning access to their own resources, introducing data in these resources and manipulating those resources), by hindering the development of information and communication technologies in countries perceived as potential enemies (which obviously includes all neighboring countries no longer under Moscow rule, but it can also include the whole world), by destroying enemy networks and information systems, and by developing information weapons and solutions to ensure the security of its own information systems. The approach is totally aggressive, offensive but contains a defensive component.

3.2.2. *The Russia–Georgia conflict*

The *Ghost Recon* video game starts in 2008 with civilian problems in Russia. Ultranationalists have taken over power in Moscow and want to restore the Iron Curtain. Their first action is to secretly support rebellious factions in Georgia and in the Baltic States. During the first missions in the game, *ghosts* must fight against rebels from the North and South Ossetia regions in Georgia, who are harassing the legitimate government and its allies, as related in the Wikipedia[34] scenario of the *Ghost Recon* video game[35], distributed in 2001. In 2008, reality seems to have partially caught up with fiction. Trying to understand and analyze this armed conflict between Russia and Georgia as objectively as possible, with its complex international geopolitical and strategic stakes, has become all the more difficult as a strong information fog clouds the landscape. There was strong mention of information, misinformation and even information warfare in this conflict in the international media as well as from the authorities of both warring countries. There was a war of

34 http://fr.wikipedia.org/wiki/Tom_Clancy's_Ghost_Recon., Video Trailer: http://www.youtube.com/watch?v=7FTzbT99-KI.

35 Developed by Red Storm Entertainment.

communications, propaganda and operations of influence. Information-in-warfare has always played a vital role. There were also cyber attacks in which both parties were victims. According to observers and direct players, cyberwar invited itself to the conflict, though denounced by the official political speech. These cyber attacks therefore should be analyzed, as should the civilian or military operations, to question their nature, origin and their place in the conflict.

3.2.2.1. *Operations in Russian and Georgian cyberspace*

From 8 August 2008, the date that we will use as the start of military hostilities for simplification purposes, many Georgian websites were defaced or paralyzed, their servers cracking under the weight of DDoS attacks. Amongst the sites affected from this date and during the following week, we find[36]:

– President Mikhail Saakashvili's website;[37]

– Foreign Affairs ministry;[38]

– The Parliament;[39]

– Ministry of Defense;[40]

– The National Bank of Georgia;[41]

– Rustavi2 television station;[42]

– sosgeorgia.org (since then, the website has a flag to inform Internet users that it is the subject of massive attacks from Russian hackers)[43].

36 Incomplete list.
37 www.president.gov.ge.
38 http://www.mfa.gov.ge.
39 http://www.parliament.ge.
40 http://www.mod.gov.ge.
41 http://www.nbg.gov.ge.
42 http://www.rustavi2.com.ge.
43 On 12 September 2008 the text said "During the last three days we have sustained massive DDoS attacks. The degree of these cyberwar attacks is unprecedented and it is possible that they will continue and maybe intensify […] it is not only an attack against our website, but war against all those who speak about the Kremlin […]".

Georgia was not the only one affected by these website-hacking operations however. The following websites were also hacked[44]:

– the skandaly.ru information website;

– the website of the Russian press agency RIA-Novosti[45];

– the Russia Today information website[46];

– South Ossetia information websites, osinform.ru and osradio.ru, where pages were replaced by those of the Georgian information agency Alania TV;

– stopgeorgia.ru[47];

– Abkhazia government website.[48]

Georgian ISPs (Caucasus On-Line and GRENA[49]) started filtering the Internet (after a government request?) to block Russian websites, as a defensive measure, in the context of the state of emergency announced by the government.

We will not include a chronological table of attacks, because it would only be useful if all the facts were listed. A partial list would only show a false representation of the tempo of aggressions and classification of targets, information vital to the search for a possible attack/counter-attack type relation. On the other hand, such a chronological representation would not be satisfied with the analysis of facts that only occurred during the few days of the armed conflict. For example, were the attacks recorded against the Georgian President's website on 20 July 2008 and against osinform.ru and osradio.ru on 5 August early warning signs?[50]

---

44 Incomplete list.
45 http://en.rian.ru/russia/20080810/115936419-print.html.
46 http://www.russiatoday.com/news/news/28835.
47 http://stopgeorgia.ru not to be confused with the stoprussia.org website, a pro-Georgian site proposing an online petition against Russian actions.
48 http://abkhazia.gov.ge.
49 Georgian Academic and Research Network.
50 DDoS attacks targeted the Web.Caucasus.net server (62.168.168.9) hosting the President's website, as well as other Georgian websites such as Social Assistance and Employment State Agency (www.saesagov.ge). It is impossible to confirm that the

3.2.2.2. *The introduction of "cyberwar" and "information warfare" in the conflict*

Georgia's Ministry of Foreign Affairs published a few unequivocal lines on its blog[51] indicating that "a cyberwar campaign organized by Russia seriously disables numerous Georgian websites, including the Ministry of Foreign Affairs website. If you cannot access the Georgian government's official websites, please go to the following websites that will provide you with the latest official information from the government of Georgia: http://georgiamfa.blogspot.com, the website of the President of the Republic of Poland, Lech Kaczynski www.president.pl (please click on the link 'information on the latest developments in Georgia')".[52] The post was titled "Cyber attacks paralyze Georgian websites".

The website of Poland's President also stated that "parallel to military aggression, the Russian Federation blocks Georgian Internet portals". It is to help Georgia, and at the request of Mr. Saakashvili, that the President of the Republic of Poland[53] agreed to make his own website available to broadcast information from the Georgian government[54].

The theory of massive attacks coordinated by Russia against Georgian information systems was relayed and supported by the words of Thomas R. Burling, manager of the American Tulip System host (a small company with a CEO, Nino Doijashvili, who is a Georgian expatriate): "We have accepted to host the President's website because Russian hackers paralyzed Georgia's Internet"[55]. The

---

Georgian President's website was specifically targeted. The attack would have come from (or gone through) the 79.135.167.22 server located in Turkey, also used to attack Georgia's parliament website.

51 http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html.

52 From 11 August 2008.

53 Remember that President Kaczynski was one of the parties involved in the liberation of Poland from Soviet rule. This hosting must be interpreted as an expression of the solidarity of Poland with Georgia. The fight of both countries is similar: the fight for freedom and democracy. Please see article http://www.latimes.com/news/nationworld/world/la-fg-media20-2008aug20,0,693386.story.

54 http://www.president.pl/x.node?id=479.

55 http://www.theregister.co.uk/2008/08/14/russia_georgia_cyberwar_latest/.

company also hosts other Georgian websites, including rustavi2 television[56].

"Information warfare" is the *raison d'être* of the very much talked about pro-Russia hacker website, stopgeorgia.ru. The site went live on 9 August 2008 and denounced information warfare operations from Georgia. It was mainly focused on operations against enemy cyberspace and proposed a list of Georgian websites that must also be targeted[57].

Cyberwar and information warfare have penetrated official political views in wartime vernacular.

3.2.2.3. *Comments on "cyber attacks"*

It is on the basis of these few official declarations and scant information relative to cyber attacks that, all of a sudden and all over the world, convinced they could see the premise of a revolutionary conflict, people in the press, on websites, in forums and blogs, used and developed this idea of cyberwar, of information warfare mercilessly fought between enemies.

Without irrefutable proof, mostly listening to their own opinions, admitting to taking the easy way out, succumbing to their fantasies, copying what others probably copied and relaying the official government speeches, hundreds of people all over the web have published their own "analyses" of the Russia– Georgia cyber conflict, proposing a vision of reality that reflects their own convictions, denouncing everyone in Russia (the military, government, intelligence services, organized crime – including the famous cyber crime network RBN[58]), in Georgia, the United States, Israel, Turkey, NATO, the real hackers, hackers in training, hacktivists, etc. The same information, for several weeks, went round in circles without leading to a convincing analysis since the situation seemed to be so confusing.

---

56 http://www.ajc.com/business/content/printedition/2008/08/17/tulip.html.
57 http://stopgeorgia.ru/?pg=tar.
58 Russian Business Network. See http://www.zataz.com/news/17611/russe–georgie–conflit–geogia–russian–cyber-blocking.html.

The media frenzy in 2008 is a reminder of the one in 2007 during the famous "Russian cyber attacks against Estonia".

Attacks against systems (telecommunications systems, networks, the Internet, etc.) that enable the transmission of official information occurred at the worst possible moment for Georgia, in the middle of the military engagement. They affected the most symbolic websites. We affect power when we attack the website of a President, a Parliament, a Ministry or a National Bank, and we affect freedom of speech, or even transfer power, when we attack the websites of some media. To deprive a government of its resources is limiting its communication capabilities, isolating it, keeping it from seeing and being seen. However, this was not the case completely. Georgia found relays, allies and alternative solutions. Its informational space was not cut off from the rest of the world. In addition to the Georgian government's websites being hosted in the United States and Poland, Estonia offered to host the websites of the Foreign Affairs Ministry, the National Bank and the Georgian civilian portal[59].

Beyond the purely symbolic aspect of the targets involved, did these attacks really have a purpose, or give the cyber attacker a significant nuisance power? Similar attacks were recorded in Russia and Georgia before the conflict and will be recorded again after. What, then, was the added value of these operations in wartime? The texts displayed on the defaced websites do not convey any message on the inter-state conflict, on the events, on tests of strength, or on the way the action was supposed to influence the course of the war; they are non-informational. The cyber attacker hiding behind those DDoS attacks and defacements reveals nothing about himself or the form of threat that he plans to use against either of the belligerents.

The attacks against information systems probably had a very limited impact on the capabilities of Georgia, because of its relatively low dependence on information systems. In fact, the

59 "Estonia hosts Georgian websites after cyber attacks", http://www.russiatoday.com/news/news/29544

network/telecommunications infrastructures of Georgia are not among the most well developed, national infrastructures are not as well linked as they are in the most advanced industrialized countries, and the population is not widely connected. Even though they are often questionable (what method was used, how were the measures defined, etc.), most indices and international classifications measuring the degree of development of nations in terms of networks, telecommunications and Internet agree on positioning Georgia among the worst students in the world. With a population of 4.6 million[60], and with only 7.49% of them being Internet users (2006 statistics)[61], the country is ranked 93rd out of 122 in the Network Readiness Index[62], behind Mongolia, Tanzania and Moldova. Estonia is in 20th position and the United States in 7th. If we refer to the series of indices published on the INSEAD website[63], Georgia is far from these model countries in terms of development of infrastructures and information and communication services. It is 100th in the E-Participation Index[64] which measures the quality and information effort made on government websites, and the services and online tools available for citizens. Georgia is ranked the same as Syria, Namibia and Burundi who are not necessarily recognized for their high level of ICT development. The "ICT Use and Government Efficiency" classification[65] (which measures the level of ICTs used by governments to facilitate interaction with citizens) positions Georgia in 96th position; Russia is 95th and Estonia is in 2nd position. The "Accessibility of public online services" classification[66] places Estonia in first position, Russia in 92nd and Georgia in 112th. The classification

60 July 2008, estimation https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html.
61 http://www.insead.edu/v1/gitr/wef/main/analysis/showcountrydetails.cfm.
62 As stated by the World Economic Forum 2006-2007 http://www.weforum.org/pdf/gitr/rankings2007.pdf.
63 http://www.insead.edu.
64 Global Information Technology Report 2007-2008, http://www.insead.edu/v1/gitr/wef/main/analysis/showdatatable.cfm?vno=9.13&countryid=340.
65 http://www.insead.edu/v1/gitr/wef/main/analysis/showdatatable.cfm?vno=9.11&countryid=340 .
66 *Idem* footnote 65.

from the ITU[67] based on the bandwidth measure for 10,000 residents puts Russia in 73rd position and Georgia in 105th position out of 127 [68].

Even though Russia is only 70th in the Network Readiness Index[69] and 82nd for the E-Participation Index (equal to Lesotho, Mali or Kazakhstan!), it still has 18% of Internet users over a population of 140 million[70], has an oversized army compared to Georgia and obviously superior information warfare means.

The impact of an attack against information systems on a population and the organization of government services is not as immediate and profound for Georgia as it would be in the case of an attack against a country that is well connected.

On the other hand, if there was an impact on websites, it could be positive. The "publicity" created surrounding these attacks made these websites gain in popularity. Who, before these attacks, was curious enough to surf the website of the Georgian President?

But the defacement of some sites, as official as they may be, clearly cannot decide victory or defeat. Could these attacks have actually favored Georgia internationally by reinforcing its image as a victim?

Attacks against information systems were not only focused on the conflict period; they also preceded the conflict. During the previous weeks, the Georgian President's website was already targeted, apparently from 20 July 2008[71]. The tensions between both countries have lasted for a long time, and the conflict was only an attempt through violence to solve the existing problem. As with any crisis

67 International Telecommunications Union. http://www.itu.int/net/home/index.aspx.
68 *Idem* footnote 65.
69 As stated by the World Economic Forum 2006– 2007. http://www.weforum.org/pdf/gitr/rankings2007.pdf.
70 https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html.
71 http://www.shadowserver.org/wiki/pmwiki.php?n=Calendar.20080720 and http://mypetjawa.mu.nu/archives/193591.php.

situation, there were manifestations of the crisis in cyberspace during the previous months and years.

Cyber attacks then became part of the conflict, "accompanied it" as some would say. A few weeks after the military conflict, cyber attack announcements became rare. There is no reason to think that these attacks will not happen again; no real solution was found, no definite agreement between Russia and NATO was ever reached. All the conditions are there for the cyberspace confrontation to continue. But it seems that the vague attempts of hackers have slowed down after 15 August 2008. Be that as it may, if cyber attacks persist, there may not be as many people willing to report them as when all media attention was captured during the week of 8 August. Other CNAs[72] will probably happen in this crisis and in the post-conflict tension phase. Regardless of the reasons for this apparent decrease of cyber attacks, it will be interesting to take a step back and observe the volumes of attacks pre- and post-armed conflict.

Similar actions (DDoS attacks, defacements) have been reported for a long time, in all countries of the region, as everywhere else in the world, especially where crises and conflicts are developing: between China and the United States, Japan and China, Russia and Chechnya, Malaysia and Indonesia, Israel and Palestine, etc. In April 2008, groups broadcasting pro-Kosovo propaganda defaced Albanian websites, and circulated lists of Albanian websites to target. In June–July 2008, 300 Lithuanian websites were defaced (with anti-Lithuanian slogans and Soviet flags[73]) following the adoption of a law banning public display of symbols dating from the Soviet era, or playing of the Soviet national anthem[74]. The recurrence of the phenomenon is such that Georgian or Russian authorities cannot invoke the effect of surprise in a context of extreme tension between both countries. There have been similarities in the processes, in the techniques used, in the logic (in a context of crisis and conflict), as well as in the nature of the targets: the website of the Georgian

72 Computer Network Attacks.
73 "Pro-Russian cyber-attack hits Lithuania", June 30, 2008. http://www.mywire.com/pubs/AFP/2008/06/30/6809382.
74 Lithuania joined NATO and the EU in 2004.

President was affected in July and August 2008, whilst in October 2007 the Ukrainian President's website[75] was also the subject of DDoS attacks[76]. In the United States, the Pentagon is constantly one of the major targets of all hackers worldwide. Political websites, as symbols of power, are obviously targets of choice.

On the other hand, confrontations in the information space are not related to time or only limited to wartime. Information attacks[77] have been the subject of squabbles between South Ossetia and Georgia for a long time. An article published on the www.civil.ge website on 14 January 2006, "S. Ossetia calls Tbilisi to Stop 'Information War'"[78], denounced information campaigns aimed at maligning the President of South Ossetia. The "information warfare" dimension, regardless of the components implemented, is part of the landscape of international relations. The element of surprise, therefore, cannot be invoked in this war situation. What can be emphasized, however, remains the state of helplessness against such operations, regardless of the author. How and why do the security systems of a government let themselves get overloaded by widely predictable cyber attacks?

The awareness of new deals in terms of information security and information systems exists in Georgia, since it is formulated in official texts, notably in the "National Security Concept of Georgia"[79], published on the web pages of the Defense Ministry site, specifically dealing with the question of information security in points 4.10 and 5.10:

– "4.10 – Information Related Challenges: Georgian national security may be put at risk because of the absence of a cohesive national information policy, weakness of infrastructure implementing such policy […]. In addition, the existence of an unsatisfactory classified information protection system, the possibility of illegal access to state information systems with the purpose of acquiring or

75 http://www.ukrainianjournal.com/index.php?w=article&id=5483, October 2007.
76 "Russian hackers cripple Yushchenko website", 30 October 2007, http://www.ukrainianjournal.com/index.php?w=article&id=5483.
77 Not only in "cyberspace", but also in the information space, in its totality.
78 http://www.civil.ge/eng/article.php?id=11511.
79 http://www.mfa.gov.ge/.

destroying information, and a likelihood of conducting large scale information attacks on Georgia from outside countries represent serious challenges to national security".

– "5.10 – Information Security Policy. […] Georgia attributes considerable importance to the protection of classified information, legal regulation of security of information technologies, and protection of the critical information systems of the state. […] the Georgian government is developing the legislative basis and infrastructure necessary for the improvement of the information technologies and secure flow of information. A Special Communications and Information Agency under the oversight of the National Security Council has been established. The establishment of the crisis management center with a situation room is under way at the National Security Council to facilitate unimpeded flow of information during the crises, inter-agency coordination and coordinated management of crisis or emergency".

The awareness of the importance of the role of information space on security and national defense expressed in these few lines does not go so far as the definition of a real information warfare doctrine, or the outline of a security strategy.

In this text, we note:

– the assertion of a defensive attitude; nothing mentions the need or will to implement explicitly aggressive processes and structures;

– the awareness of the threat that superiority of information of potential enemies may represent;

– the identification of information warfare threats: CNA ("intrusions", "large scale attacks"…), ISR ("classified information", "illegal access"…), etc.;

– a methodology that gives the government control in terms of security and defense, but that does not seem to partner with the private sector (the text is probably too short to offer this direction).

Even though the attacks against Georgian and Russian information systems are part of the conflict, the identity of the (guilty) authors of

these acts remains difficult to confirm. It would appear that accusing the direct enemy is legitimate, as the Georgian government is doing. The reality may be more complex but the accuser does not really have to worry about the validity of his comments, or the verification of the facts. The accusation must serve political, ideological and partisan interests.

The servers involved were in Russia, Turkey and the United States… Beside the military or governments, we could reasonably think that hackers driven by a patriotic feeling (hacktivists) were involved:

– Who is the famous "South Ossetia Hack Crew" claiming the defacement of the Georgian Parliament's website that nobody has ever heard about? Who is behind the "FeDeRer & Terrorists" signature claiming the defacement of the Interior Affairs Ministry police.ge on 5 August 2008? Who is "P47RICK" signing the defacement of the http://saagento.security.gov.ge website? Or who is SinqRonize, the author claiming responsibility for a simple "NO WAR! Fuck Russia:) For Türkiye..." the defacement which appeared on kavkazblog.com? Even if they are "signed", these actions remain anonymous because the signatures are worthless. They can hide an individual or a group; several signatures can hide a single individual, etc.

– Must we speak of Russian or Georgian actions? It is impossible to get precise information about the real identity of the authors of such CNAs.

Defacements have mainly consisted of replacing official pages by photomontages associating the image of the Georgian President with Hitler. Such images are found on the Flickr.com website[80] and several forums in which there is not really a debate but rather where a bunch of scathing insults are exchanged. The war.georgia.su website, which denounces Georgian misinformation with videos as proof, presents the Georgian President as a Nazi. Saakashvili is said to use the same methods as the Nazis, wear the same clothes, etc. The website demonizes the enemy: "They have pity for no one, killing women,

80 http://flickr.com/photos/27074615@N06/2755219768/ and http://flickr.com/photos/75255787@N00/2753053679/.

children and older people ... the wounded were struck with bayonets... some were burned alive in their homes...". A "genocide", a "holocaust" was committed, 3% of the population was decimated in one night, etc. Russian troops are presented as peacekeeping forces, Georgian operations as war crimes. This demonization has many effects including putting an enemy out to pasture in front of international opinion to weaken him, tarnishing his image, and clearly justifying the demonizer's own actions as well. Against enemies fearing neither God nor man, without morals, is not everything allowed? Hacker operations even seem legitimate, without even any questioning of the morals and legitimacy of their action.

Associating the image of authorities with 20th Century dictators is not specific to the Russian–Georgian conflict. There have been associations made of the images of Hitler and Mussolini to George W. Bush[81], of Hitler to Putin[82], etc. Armenia (pro-Russia) uses this comparison when it speaks of Azerbaijan. According to an article published by the Armenian website www.novarak.am[83], Azerbaijanis used the same methods as Hitler and Goebels: lying or telling the truth is irrelevant, the important thing is to be the first to talk, knowing how to manipulate national and international public opinion[84], being present in international organizations under the pretense of democracy, supporting information by reference to individuals with authority, whether they exist or not, institutionalizing the lie, changing the image of the enemy in the eyes of public opinion, etc. Azeris Day.az, ANS and APA press agencies seem to be the players of this institutionalized misinformation. We have been recording exchanges between Armenian and Azerbaijani hackers for many years now. In 2000, we registered the attack of dozens of Armenian websites located in Armenia and in the United States by Azerbaijani groups with names

81 On http://www.thepeoplesvoice.org/cgi-bin/blogs/voices.php/2008/08/, see the image posted 3 August 2008.

82 http://www.flickr.com/photos/teonna/2756230123/ or http://www.rgnpress.ro/Politic/Putin-=-Hitler.html.

83 www.novarank.am/en/?page=print&nid=1203.

84 Defining "public opinion" is a very difficult task. We just have to recall that for Pierre Bourdieu "Public opinion does not exist", *Temps Modernes*, 29 (318). January 1973. pp. 1292–1309. The text is available at the website http://www.homme-moderne.org/societe/socio/bourdieu/questions/opinionpub.html.

such as “Green Revenge”, “Team of hijackers-187”, etc. involving the Nagorno–Karabakh situation. Armenian groups were also active as “Liazor”. Conflicts for the sovereignty of territories are the cause of these outbreaks[85].

The Georgian government chose to discuss the cyber attack aspect of the conflict, and to use these aggressions against its cyberspace to denounce enemy operations, accuse Russia, and thus reinforce its image as the victim (justifying self-defense) which it has circulated in its communication campaign directed at national and international public opinion. Although cyber attacks are no longer a new phenomenon in the context of international conflicts and crises, the condemnation of these operations and their use for communication purposes is significant. This methodology was used by Estonia in 2007, where that country widely denounced the cyber attacks against it, accusing Russia, and focusing the attention of the international community on its status as a victim without providing more details on the nature of the attacks and the targets really affected.

The sentences in the texts published on government websites are structured similarly to what is written on Georgiamfa.blogspot.com by the Georgian Foreign Affairs Ministry: “Cyberwar attacks conducted by Russia disrupt Georgian websites; the Georgian government has implemented replacement sites”. In the structure of this sentence, as in the others, we find the following information elements:

– action (cyberwar attack);

– author (Russia is the accused);

– impact of the attack: websites down;

– victim: Georgia;

– subject of the new action-reaction: Georgian government;

– action-reaction: solutions of substitution, compensating for damages (reaction to impact), verbal accusation (reaction to attack)

85 www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=141 “Back files: computer specialists urge end to Armenian-Azeri hack attacks”, 18 February 2000.

and online publication of this short sentence (action, aimed at national, and especially international, public opinion).

All the sentences are accusatory. The enemy is presented as the first attacker. Georgia is only reacting defensively. Cyberwar is not a theoretical threat, it is real. With very similar words and in a slightly different order, the texts published by the government, and the comments from the host Tulip System transmit the same message and contribute to building the image of a victimized state with its democracy being attacked.

Outside of the conflict itself, as with any extraordinary event, information is used by cyber criminals, taken out of context and used as a lure. Spamming using known information to lure the user is not new, and it is already detected by Symantec[86]:

– "Russia–Georgia conflict news used to hide malicious code in spam"[87]. Symantec identified viral spam disguised in an information article involving the Russia-Georgia conflict. The subject of the message was "Journalists Shot in Georgia". The message contained an attachment with a password and instructions to download a file. The user was actually redirected to a payload identified as the Trojan.Popwin virus. This is using false information to attract the user in an operation that will be harmful. Protection against these viral spams involves using anti-virus software and common sense.

– Another example detected by the University of Birmingham (Alabama, USA)[88] is the viral spam that sends you, through a link, to false information from the BBC saying that the Georgian President is gay (19 August 2008). The spam servers were on Russian territory, one of the machines was even part of the Federal Education Agency. According to the article published in vnunet, the virus would add

86 http://www.symantec.com.
87 https://forums.symantec.com/syment/blog/article?blog.id=spam&message.id=111#M111 21 August 2008.
88 Related in http://www.crime-research.org/news/19.08.2008/3521/.

affected computers to botnets under pro-Russian control and would also contribute to the anti-Georgian propaganda[89].

3.2.2.4. *Isolated cyber attacks or information warfare operations?*

Information warfare operations can be conducted by an impressive range of players with the most varied potential, whether they are carried out by military or civilian players: States, the military, structured groups (terrorists, rebels, activists etc.), isolated individuals, or simple computer "hackers". Their motivations can be political, economic, ideological, etc.

Were the actions qualified as cyber attacks only carried out by hacktivists? Are hacktivists always civilians?

The stopgeorgia.ru website calls for actions in cyberspace in defense of Russia: "We, representatives of the underground world of Russian hackers, will no longer tolerate Georgian provocation in any form. We want to live in a free world without attacks […]. We do not need to be guided by authorities or anyone, but act according to our convictions based on patriotism, conscience and trust by virtue of justice. You can call us criminals and cyber terrorists […] but we will fight in Cyberspace against the unacceptable aggression of Russia. We demand the end of attacks against information and government resources, and call for all media and journalists to cover the events objectively. Until the situation changes, we will stop the dissemination of false information […] We did not start this information warfare, we are not responsible for its consequences. We call for assistance from all those concerned with the lies from Georgian government websites…"[90]. The website offers a list of the main official Georgian resources[91] without publishing hacking tools. But by naming targets, the objective is to facilitate the job for hackers. The homepage offers links to websites (war.georgia.su and www.stop-war.us) sharing the same concern for condemning Georgian misinformation. The "media-lies" section of the war.georgia.su website denounces the media

89 http://www.crime-research.org/news/19.08.2008/3521/.
90 Text available on the homepage of the stopgeorgia.ru website.
91 http://stopgeorgia.ru/?pg=tar.

manipulation, the doctored pictures from the Reuters agency, the distribution of false information from a press agency, and the use of this same false information by international media.

These websites and the individuals hiding behind them contribute to information warfare (giving their interpretation of reality[92], of the truth, or by feeding confusion), and to information warfare in its CNA dimension. They claim their independence, their freedom of action and speech. But as for their real nature, anything could be true. They may not be as independent as they pretend to be.

Were the actions qualified as cyber attacks carried out by the military? Was their use of information warfare methods to prepare confrontations, cut off enemy networks, blind the enemy, cover missions on the field by prior computer strikes? What military use was really made from information warfare in this blitzkrieg? Have the Russian and Georgian governments, beyond the regular psychological confrontation (information, misinformation), used network attack methods, interception of communication, or physical attacks against communication infrastructures to ensure control of the information space?

The Russia–Georgia conflict probably provided its belligerents with a field of use for their information warfare capabilities. However, the absence of information from Russian and Georgian military operations prevents any definite conclusion and any methodical analysis. There is nothing to help us confirm that the attacks against Georgian information systems were a coordinated action by the Russian military in order to cut off the communication systems of the country and facilitate the progression of military operations; but there is nothing to enable us to deny it either. The few temporary site defacements and overloading of servers, to which replacement solutions were quickly found (mirror sites, website hosting from allied countries, etc.) do not add up by themselves to the concept of information warfare.

92 On the concept of "reality" remember the work of Paul Watzlawick *La réalité de la réalité. Confusion, désinformation, communication*, Le Seuil, Paris, 1984.

3.2.2.5. *Formulating the right questions*

It is probably too early now to rebuild the scenario of what really happened in the information space of the belligerents and draw conclusions.

Time will be needed for an investigation and methodical analysis that will prevent us from falling into the trap of the media fad, by focusing on the following questions specific to this conflict, and then to the more general and conceptual:

– Could this "information warfare", as this is the expression used, be summed up as a few defacements and breakdowns of official Internet websites?

– What actions in cyberspace must be defined as acts of war, and which ones are only acts of delinquency?

– Do the confrontations reveal the existence of a cyberwar arsenal?

– Is it possible to reconstitute the tempo of aggressive and defensive operations from both parties and draw general conclusions on the role played by the 4th combat dimension in a blitzkrieg? Can this role be marginal or must it be central?

– What actions were conducted under army or government control?

– Did the army really seize the information space, or cyberspace, to carry out this Blitzkrieg? What information warfare operations did the military really carry out? What is new in the way this war was conducted?

– Were citizens (Russian, pro-Russian, Georgian or pro-Georgian) involved in the cyber conflict? Could the "people's war" concept, dear to the Chinese, win the world? Could we eventually see a new type of citizen of the cyber combatant world? Nothing is more questionable. Hacktivists invite themselves to all crises and conflicts without their actions having any proven influence on the course of events so far. The masses of defacements are often the work of a few rare hackers who cannot alone authorize the use of expressions such as "people's war", supposing the investment of a significant number of individuals.

– Would the participation of civilians in conflicts be an asset or would it contribute to the increase of the information fog? If this participation proved to be harmful to success, would it be possible to contain it? Would the participation of civilians influence the international strategic balances of power?

– What are the relations, if they exist, between organized crime and war effort in cyberspace? Did the involvement of the RBN in cyber attacks against Georgia really happen?

– What would the relationship be between civilian and military worlds in the 4th dimension of combat constituting the information space and particularly cyberspace? Could the States consider using Private Military Societies (PMS) to conquer the field of cyberspace? Could the experience acquired by cyber criminal groups enable a temporary conversion into cyberspace PMS? The expansion of the use of PMSs would then only be the extension of the privatization of violence. The reflection will then involve the role that PMSs could play in information warfare, as well as on risks that the States would incur with the uncontrolled use of such players, and on the acceptable limits of the challenge of the monopoly and the control of violence by the Nation-State (the Westphalian order).

– Does a "game-playing" dimension not appear in the war when simple hackers can benefit from a context of chaos to interfere, increase confusion by their actions, make the enemy think of acts of war, and take the appearance of great powers? Or when official war players (the military and governments) can make people think it was the action of ludic hackers to hide their operations?

– When server and site hacking does not disrupt, in a significant way, the operation of armed troops, does not penetrate and disrupt the C4ISR communication systems, does not affect the systems ensuring the operations of sensitive infrastructures, and does not jeopardize the communication systems ensuring the management of crisis and emergency situations, should we be worried about actions from hackers/hacktivists defacing or taking down general information, and even official, websites? In this conflict, hacking a few websites has taken on a media importance that is out of proportion, with no relation

to the real consequences of the facts. Who has really benefited from the media sound box?

– What has been the impact of defacements and decommissioning of official sites?

– Is the advantage gained by the offensive in terms of cyber aggression unstoppable?

– Must we give a strategic and political importance to operations that are not claimed?

– What dimensions of information warfare are real power intensifiers? Does information warfare confer an advantage leading to success?

– Isn't the control of the information space wishful thinking?

– Can a modern war, blitzkrieg or long term, be won without using information warfare?

– To what does Russia owe winning the war? To its lethal kinetic actions or an information warfare advantage?

– Several categories of websites were affected: governmental, as well as hacker, commercial, media, etc. Is the impact on the conflict different according to the nature of the target?

– Must we know how to maintain hacking in peacetime to be able, when the time comes, to mobilize it with nationalist feelings? Can the hacker and hacktivist be manipulated?

– What alternatives exist, in terms of cyberwar and information warfare, to expensive American solutions? Is a cheaper cyberwar, far from the staggering costs involved in programming, planning and implementation of grandiose American cyberwar programs, possible?

Georgia is a nation that has too much vested in cyberspace for the few aggressions experienced (summed up as a few server and Internet website attacks) to appear as a massive information warfare operation. In this short period of asymmetrical war, Russia won a victory, but we still do not know, because of lack of information, the real importance that information operations have, and if the fight for the control of the information space is predominant. Of course, in the traditional sense

of the term, there was information warfare, since warfare information and information-in-warfare were discussed, i.e. the use of information to recount events ("stories"?[93]), to play with opinion, influence, rally to its cause part of the rest of the world, denounce, i.e. conduct psychological operations. However, in terms of Cyber attacks within the Russia–Georgia conflict, we would be tempted to conclude that they simply constitute a non-event.

3.2.3. *Ukraine*

This serious crisis provided a field of application for the actors themselves involved in information warfare, and a field of observation for strategists and researchers the world over. "Russian information warfare in Ukraine" has become a genuine subject of study.[94] The Russia–Ukraine crisis has become the archetype of "hybrid conflict", which denotes conflicts where kinetic actions have the same degree of importance as cyber warfare and information warfare actions.

The Ukrainian scenario in 2014 took place in two stages: the first, founded on an international issue, centered on the demonstrations and armed conflicts between the population and those in power; and the second centered on the annexation of Crimea by Russia.

It was on 24 November 2013 that what was to become the largest demonstration in the country since the Orange Revolution of 2004[95]

---

93 Christian Salmon, *Storytelling, la machine à fabriquer des histoires et à formater les esprits*, La Découverte, 2008.

94 Pille Pruulmann-Vengerfeldt, How to Analyse Information Warfare: the Case Study of Russian Propaganda Tools in Ukraine, Estonian National Defence College & University of Tartu, 2015, 27 slides: http://www.baltdefcol.org/illc2015/wp-content/uploads/2015/06/13.-M%C3%BC%C3%BCr.pdf.
Stefano Lupo, La dimensione russa dell'information warfare in Ucraina, Osservatorio di Politica Internazionale, Research Paper no. 18, June 2014, 15 pages: http://www.bloglobal.net/wp-content/uploads/2014/06/La-dimensione-russa-dellinformation-warfare-in-Ucraina_Research-Paper_Lupo_giugno-2014.pdf?3008ee.

95 In November 2004, the victory of Viktor Yanukovych in the presidential elections was announced. A vigorous protest movement arose to contest that victory, which was felt to be fraudulent. The opposition managed to obtain a third count, which then unseated Yanukovych and declared Viktor Yuschenko the winner (in December 2004). This phase of contestation is known as the Orange Revolution. Researchers

took shape. Over 100,000 people demonstrated in Kiev, demanding that Ukraine be allowed to become part of Europe. The occupation of Maidan Nezalezhnosti (Independence Square) began on 30 November 2013. On 22 January 2014, three protestors died in clashes with police; the bloodiest day of the conflict was 21 February. The President abandoned the capital and was then removed from office on 22 February.

On 27 February, armed men seized the Crimean Parliament building, and raised the Russian flag. On 11 March, the Parliament of Crimea voted for the independence of the Autonomous Republic of Crimea. On 16 March 2014, it was decided by referendum that Crimea should attach itself to Russia, which was made official by Moscow two days later.

In cyberspace, the protagonists of these crises were numerous. They include civilians who reported/witnessed the events, the traditional media, cyber crime hackers, the hackers of the State forces, hacktivists (nationalist/patriotic hackers, both pro- and anti-Russian/ Ukrainian/European/governmental, etc.). Behind the signatures, tags, labels and demands displayed, their true identities may well be lost in the labyrinthine expanse of cyberspace. The risk of manipulation and of disinformation is high. Therefore, it is difficult to conduct an analysis. With regard to the events in Ukraine, from November 2013 onwards, the international media have all been repeating information that tends to show that networks are at the heart

---

have analyzed the role played by the Internet and mobile telephony during the Orange "Revolution". They demonstrated that these tools had indeed been used, but were unable to categorically conclude that they played a determining role in the course of events.

Joshua Goldstein, *The Role of Digital Networked Technologies in the Ukrainian Orange Revolution*, Internet & Democracy Case Study Series, Harvard University, December 2007, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf

Myroslaw J. Kyj, "Internet use in Ukraine's Orange Revolution", *Business Horizons*, Elsevier, United States, no. 49, pp. 71–80, 2006,

Adrian Karatnycky, "Ukraine's Orange Revolution", *Foreign Affairs*, 84 (2), March-April 2005.

of the events. Below is a list of the main facts reported by the international media.

Operations by hacktivists from Russia, Ukraine and potentially many other countries targeted the websites of the authorities, media institutions and companies.

The crisis with Ukraine was accompanied by actions in the cyber/information space. A few examples are:

– attacks on the telecommunication networks. In 2013, we saw the exploitation of the telecommunication infrastructures by Yanukovych's (pro-Russian) government, to send messages directly to the protestors' mobile telephones[96];

– attacks on the mobile phones of Ukrainian Members of Parliament;

– DDoS attacks;

– website defacement (attacks by pro-Russian and pro-Ukrainian hackers on enemy Websites);

– deactivation of the Ukrainian government's website 72 hours after Russian troops entered Crimea on 2 March 2014;

– hacking of the computers and servers (using the malware tool Snake) of the Ukrainian Prime Minister and various Ukrainian embassies throughout the world;

– when monitoring the Ukrainian presidential elections, in March 2014, the Ukrainian security services discovered the presence of a virus in the systems of the Central Election Commission (intended to sabotage the processing of the votes). Responsibility for the attack was claimed by the group CyberBerkut;

– in view of the actions by hostiles, support measures were taken by other countries: thus, Ukraine received support from NATO (by

96 The Russia–Ukraine conflict: cyber and information warfare in a regional context, ETH ISN Zurich, 17 October 2014: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=187945&lng=en.

way of 20 million USD financial aid in non-lethal defensive resources – particularly in terms of cyberdefense);[97]

– Cyber attacks against the Russian media (Russian Channel One attacked by Anonymous Caucasus), against the websites of the Kremlin and the Central Bank;

– the operations of a group of pro-Russian hackers, signing themselves as CyberBerkut[98], claiming responsibility for, amongst others, the attack on three of NATO's websites – the main site (nato.int); the websites of the CCD COE in Tallin (ccdcoe.org); and the site of the NATO Parliamentary Assembly (nato-pa.int)[99]. NATO reported that the incidents did not have any lasting consequences[100]. The group declared on its website that it did not accept the presence of the NATO occupying force on Ukrainian soil. Since the end of the riots, the group's stated objective has been to combat the neo-fascist propaganda of the media which it deems corrupt[101]. The group has its own website[102] and Facebook page[103]. It is believed to be responsible for over 100 hack attacks on Ukrainian websites;

– interference with Ukrainian telecom systems has been reported. The main telecom provider in Ukraine, Ukrtelecom, declares that it was the victim of sabotage operations in Crimea, in late February 2014[104]. Renesys[105] was unable to verify the accuracy of this report. At

97 *Idem* footnote 96.

98 This is the name of a special police force within the Ukrainian Ministry of the Interior, which employed terror methods to fight the opposition to Yanukovych.

99 http://rt.com/news/nato-websites-ddos-ukraine-146/.

100 Declaration by the NATO spokesperson, Oana Lungescu, on Twitter on 15 March 2014: "Several #NATO websites have been target of significant DDoS attack. No operational impact. Our experts working to restore normal function", http://rt.com/news/nato-websites-ddos-ukraine-146.

101 http://rt.com/news/nato-websites-ddos-ukraine-146.

102 http://www.cyber-berkut.org/. According to the statistics produced by Alexa (request made on 30 March 2014: [http://www.alexa.com/siteinfo/cyber-berkut.org]), nearly 58% of the site's visitors are Russian, and fewer than 15% are Ukrainian.

103 https://www.facebook.com/CyberBerkut.

104 J.C. Finley, *Telecom services sabotaged in Ukraine's Crimea region*, UPI.com, 28 February 2014, [http://www.upi.com/Top_News/World-News/2014/02/28/Telecom-services-sabotaged-in-Ukraines-Crimea-region/7611393621345/#ixzz2uwG5pVPN].

most, the analyses illustrate a disturbance of 5 hours. Hence, this incident is not a significant one, and does not conclusively demonstrate the occurrence of an attack (by the Russians or others) against the telephony services. In early March 2014, the Ukrainian security services reported Cyber attacks against the country's telecom systems, apparently originating from installations in Crimea. The resources deployed, notably, would enable the attackers to interfere with parliamentarians' mobile phones. Equipment to block communications appear to have been installed at the input points to the network of the operator Ukrtelecom in Crimea[106];

– the virus *Snake*, which has been active for many years, appears to have infected Ukrainian government networks in 2013, according to a study by BAE Systems. Of 44 recorded cases of infection throughout the world since 2013, 22 are in Ukraine, which thus appears to be the primary target[107], with the rate of infection increasing since January 2014;

– finally, studies seem to demonstrate that social networks, through their main applications which are Twitter and Facebook, prove to be an essential tool in the service of the demonstrators[108], and thus doubtless as well for the authorities (when they are capable of monitoring these communication spaces, infiltrating them, and analyzing the information gleaned from them). As the majority of exchanges over Twitter are in English, queries have been raised: have the Ukrainians decided to write in English in order to attract the attention of a wide international community? Do foreign actors account for the majority of exchanges on Twitter? However, on Facebook, the most active page (https://www.facebook.com/

105 https://twitter.com/renesys/status/439526174771773440/photo/1.

106 Jerin Mathew, "Equipment Installed in Crimea to Tap Lawmakers' Phones: Ukraine Security Services Chief", *International Business Times*, 4 March 2014, http://www.ibtimes.co.uk/equipment-installed-crimea-tap-lawmakers-phones-ukraine-security-services-chief-1438821.

107 "L'Ukraine cible d'un puissant virus informatique", *Le Monde*, 9 March 2014, [http://www.lemonde.fr/technologies/article/2014/03/09/l-ukraine-cible-d-un-puissant-virus-informatique_4380014_651865.html].

108 Pablo Barbera, "Tweeting the Revolution: Social Media Use and the #Euromaidan Protests", *Huffington Post*, 31 March 2014, [http://www.huffingtonpost.com/pablo-barbera/tweeting-the-revolution-s_b_4831104.html].

EuroMaydan) is written entirely in the Ukrainian language, and is thus more operational for the actors on the ground (seeking volunteers for hospitals, information about the wounded and dead, etc.). The Facebook pages publish images of violence. Social networks tell the story of the combatants/demonstrators[109].

Ukraine, in conflict with Russia, is *a priori* in a situation of major asymmetry if we look just at the level of its state (military) forces. The Ukrainian cyber crime component, though, proves to be a possible variable in solving the problem, in addition to which we must consider the support received from foreign nations. Yet there is nothing to prove the mobilization of cyber criminal networks by the Ukrainian state.

On the other hand, as regards Russia, the analyses formulated by Jeffrey Carr suggest that the situation has changed since Putin's accession to power. In the past, there have been cyber criminal groups (the most famous of them being Nashi), calling for attacks on adverse countries, quick to act on behalf of Moscow, as was the case in 2007 (attacks on Estonia) and 2008 (attacks on Georgia)[110]. That is no longer the case. There may even be factions in the community of Russian hackers who do not support the Putin government's action.

Ukraine, whose cyberspace has greatly changed over the course of the past 10 years (the Internet penetration rate has risen from 3% to 40% of the population) has been the theater of revolts and major political crises. Nonetheless, it is tricky to measure the true weight held by cyberspace in the ratios of force, and particularly the advantages lent to the various actors, expressed in political terms. It proves highly risky to establish a direct link between political change and mastery of the technologies and of the information space, and if it were the case, more

109 John Bowman, 'Face of Ukraine': Maidan protesters' stories told on social media, CBC News, 19 February 2014, [http://www.cbc.ca/newsblogs/yourcommunity/2014/02/face-of-ukraine-maidan-protesters-stories-told-on-social-media.html].
110 Jeffrey Carr, "Russian Cyber Warfare Capabilities in 2014 (We aren't in Georgia anymore)", *Digital Dao*, 8 March 2014, [http://jeffreycarr.blogspot.fr/2014/03/russian-cyber-warfare-capabilities-in.html].

specifically between a political effect and a particular type of technology or operation. For the main protagonists, the defensive/ offensive use of cyberspace constitutes a veritable challenge: because the adversaries' intentions are always difficult to anticipate; because the true level of capability of states in terms of cyberdefense is not well known; because an international judicial framework is already lacking. The limits on the use of cyberdefense capabilities are, aside from the technique, those which states impose on themselves, in terms of law, ethics, risk evaluation and the desired effects.

3.3. Comments

3.3.1. *Characteristics of the Russian idea of information warfare*

Definition	Date	Source
"Information warfare is a way of resolving a conflict between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/ psychological and information/ technical influence on a nation's decision-making system, on the nation's populous [sic] and on its information resource structures, as well as by defeating the enemy's control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets".	May 1995	Remarks by a Russian officer, quoted in Timothy L. Thomas, 1996[111]
"Within the framework of the execution of the operational-strategic (operational) missions of offensive	May 1995	Remarks by a Russian officer, quoted in Timothy L. Thomas, 1996[112]

111 Timothy L. Thomas, "Russian views on information-based warfare", *Airpower Journal*, 1996, pp. 25–35, USA: http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spec96/thomas.pdf.
112 *Idem* footnote 111.

and defensive troop units, information warfare consists of the specially planned and coordinated-integrated actions of the forces and assets of intelligence and early warning, command and control, communications, deception and electronic warfare, whose purpose is to guarantee the achievement of the goals of the operation (of its combat actions)"		
"In the broad sense, information warfare is one of the varieties of the cold war counter – measures between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people's public/social awareness, to state administrative systems, production control systems, scientific control, cultural control, and so forth. In the narrow sense, information warfare is one of the varieties of military activity/operations/actions (or the immediate preparation for them) and has as its goal the achievement of overwhelming superiority over the enemy in the form of efficiency, completeness, and reliability of information upon its receipt, treatment, and use, and the working out of effective administrative decisions and their purposeful implementation so as to achieve combat superiority (victory) on the basis of this".	September 1995	V. I. Tsymbal[113]
Information war is the "Confrontation between two or more states in the information space to damage the	2011	Conceptual Views Regarding the Activities of the Armed Forces of the Russian

113 *Idem* footnote 111.

information systems, processes and resources, which are of critical importance, and other structures, to undermine the political, economic and social system, and effect massive brainwashing of the population for destabilizing the society and the state, and also forcing the state to make decisions in the interests of the confronting party".		Federation in the Information Space (2011)[114], Cited in Eve Hunter, 2015[115]
"a kind of warfare between parties in which special (political, economic, diplomatic, military, and other) methods and measures are used to influence the informational environment of the enemy, and to defend one's own environment in order to achieve one's defined goals	2012	Igor Panarin[116]

Table 3.4. *Russian definitions of information warfare/information war*

3.3.2. *Aggressiveness*

Information warfare is a conflict in the information space. It is mainly considered a form of military operation that must be under the responsibility of the Department of Defense. The Russian concept is aggressive and offensive. The idea is to control and, in order to succeed, to destroy, disorganize and damage. Information systems and information (attack of C2 systems, cyberwar consisting of the use of

114 Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, 2011: https://ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf.

115 Eve Hunter, Piret Pernik, The Challenges of Hybrid Warfare, International Centre for Defence and Security, Tallinn, Estonia, p. 7, April 2015, http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf.

116 Igor Panarin, "The doctrine of Russia's information warfare", 2012, cited in Jolanta Darczewska, "The devil is in the details. Information warfare in the light of Russia's military doctrine", *Point of View*, no. 50, Warsaw, p. 39, Center for Eastern Studies, May 2015.

hacker techniques), and individuals, in their psychological and physical dimensions, are the target of this aggressiveness.

Yet the technique is, of course, also defensive.

In 2001, Sergei Ivanov[117], Minister of Defense, defined information warfare as the series of actions taken by a country to damage the resources and information systems of another country while protecting its own infrastructure.

3.3.3. *Type of Cold War*

In its strategic dimension, information warfare is perceived as a type of Cold War[118]. Cold War is defined as the implementation in peacetime of counter-measures between two governments, such as counter-psyops and counter-intelligence. The Russian military extends information warfare methods into peacetime, in the same way as the Americans did with their concept of information operations. Extending operations into peacetime also means that the military does not work alone in information warfare missions. Intelligence agencies, for example, may have to act in this context, since their role is to carry out counter-intelligence actions and collect open or hidden information on any potential enemy.

Information warfare is not a substitute for other forms of warfare. It complements them even though it is sometimes perceived as a totally new form of warfare, as expressed by General N.A. Kostin[119], and can be conducted in peacetime and wartime.

The expression, Cold War, obviously brings back the threat of a nuclear war. The link between the two types of war was established

117 C.G. Billo, W. Chang, *Cyber Warfare, An Analysis of the Means and Motivations of Selected Nation States*, Institute for Security Technology Studies, Dartmouth College, December 2004, 142 pp. http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf.

118 Dr. V.I. Tsymbal, a Russian analyst.

119 Quoted in T.L. Thomas, "The Russian view of information war", in *The Russian Armed Forces at the Dawn of the Millennium*, Critcher Michael H. (ed.), December 2000.

when Russia said it would respond with nuclear power if it was a victim of an information warfare-type attack [THO 00].

3.3.4. *Challenges, objectives and targets*

Information warfare must have specific objectives. It provides the means and methods to reach these objectives.

The challenge is to be able to influence the information resources of the enemy (Admiral Vladimir Semenovich Pirumov)[120] while protecting our own. This is the approach traditionally adopted in the definitions of the American model. Beyond this basic challenge lies a specific objective.

Information warfare therefore remains only a means, like any other, to reach one or more objectives, and it is not a substitute for other forms of warfare.

Influencing the information resources of the enemy must enable us to achieve our first objective, which is reaching and maintaining an advantage over information in relation to the enemy[121], to the benefit of our own C2s. C2s must have the best quality and most precise information possible. There is a common idea: see first, see better and act before the enemy. The objective then is clearly to improve our own capabilities to close to the OODA cycle while disrupting the enemy's. The observation and orientation phases require work before the conflict, with intelligence (acquisition of information on the enemy and allied troops), information counter-measures (blocking the enemy's collection and processing of information), information defense measures, deception and information sharing between both levels of C2. A government cannot think about the improvement of these two phases when a war is launched. The advantage acquired will then be made a reality in the decision and combat action. According to the Russians, countries with superiority of information are more liable to use military force than in the past.

120 Quoted in T.L., Thomas "Dialectical versus empirical thinking; ten key elements of the Russian understanding of information perations", *The Journal of Slavic Military Studies*, http://leav-www.army.mil/fmso/documents/dialect.htm,1998.
121 Colonel S.A. Komov, Russian military thinker.

This advantage over information must be acquired by aggressive methods. According to Colonel General Valery Manilov, Chief of Staff of the Russian army (1996–2001), information warfare is a fight within or between governments, which must use very aggressive methods to damage or completely destroy the information space of the enemy camp. The information space here is meant in a wide sense and not only military. All spheres of social activity are included in this expression and subjected to this informational influence. The possibility of conducting information warfare within a government must also be considered.

The challenge is controlling what Russians call the space, or environment, of information, defined as a very large whole, not completely military or civilian. It includes everything, it is the sum of all a government's databases, infrastructures and methods of collecting, processing and broadcasting data, i.e. infrastructures of telecommunications, networks, terminals and satellites, everything that enables the interaction between information and organizations and citizens, and the satisfaction of their needs in terms of information[122]. It is a space that includes all the players in a nation (individual citizens, corporations and government organizations), who act on information (collect it, process it, manage it, use it and exchange it) in a space that is more than just virtual. Networks, infrastructures and communicating tools are the physical space that makes up the backbone of this informational space enabling information flows (transmission, storage, processing, interpretation, displaying, representation and perception). This information space is therefore a single entity and is global. Information resources are the raw material of this space. They include all the data acquired, processed and stored in all human activities including science, economics, politics, culture and information received daily by citizens and the government. We speak of resources because this data, once stored, can be delivered anytime and anywhere depending on the needs and requests of their users.

Within this information space and information resources, sub-spaces and blocks of resources are identified and must be the subject of specific security. All infrastructures and all sets of information do

122 R.M. Yusopov, *Information Security is the Foundation of National Security*, Vooruzheniye, Politika, Konversiya, nos. 3–4, pp. 35–38, March–April 1997.

not have the same degree of strategic importance. Government C2s or those of the military, financial and banking systems, transportation and energy infrastructures and alarm systems, are all vital infrastructures and should be protected by higher security. The global security of the information space remains one of its major problems.

Rafael M. Yusupov, SPIIRAS Director[123], estimates that the two major threats to this space are espionage and information distortion, two actions that can occur during times of peace. Other threats were identified by the government: intelligence gathering, electronic warfare, systems intrusion, terrorism, cyber crime and psychological operations – a major concern – via possible operations from foreign groups against Russia, or from internal propaganda activities against the government. We must not forget human error in sensitive information systems. There is no perfect solution for real protection of this information space.

The information space and information resources are the two major principles in the Russian doctrine of information control and information warfare. Space is simultaneously the key structure of a government and the target chosen to disrupt the global balance of power of that government. The concept of information control extends to the global control of information space and all resources, even overflowing from a period of crisis and conflict into a period of peace. There is no major difference with the American ideology. Any information can be strategic and sensitive; the information environment is global and its control can be problematic, but it is a major, given, challenge. However, the desire to meet this challenge has only surfaced in recent conflicts.

There are a number of examples of the way the notion of "control of information" was handled in the conflicts conducted by Russia in the last decade. During the Chechnya conflicts[124] after 1994, Russia confronted an enemy that also had cyberwar capabilities and could use

123 St Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, www.spiiras.nw.ru/index.php?nawlang=english.

124 Yusopov R.M., *Information Security is the Foundation of National Security*, Vooruzheniye, Politika, Konversiya, nos. 3–4, pp. 35–38, March–April 1997.

its capacities to dominate the informational world. In the first Chechnya war (1994–1996), meant to restore Russian order, Russia's strategy in terms of dominance of the information space focused on banning the press from following and reporting the conflict in the national and international media. It hoped to control all the information entering and exiting the space of conflict. Instead, Chechens used the media to spread their message across the international community. Information warfare in this first phase took the form of psychological operations, operations to influence public opinion through the media. Whilst the Chechens learned the lesson from the war conducted by the Americans in the Gulf, the Russians apparently did not. Not simply for this reason alone, the first Chechen conflict resulted in a Russian failure, but it illustrates the possibility of a digitally weaker adversary holding a superior enemy in check (in an asymmetrical war) by avoiding symmetrical confrontations, frontal attacks and by using the enemy's weak spots to strike. The information space was one of the weak points of the Russians during this first conflict, and Russian public opinion was one of Chechnya's preferred targets. Nevertheless, the Russians were still able to use information technology methods during the war: in 1996, Dzhokhar Dudayev, the leader of the Chechen rebellion, was located by the Russians through a call he made from his satellite phone and killed by a precision guided bomb.

During the second conflict (1999–2000), officially motivated by the fight against anti-terrorism, the Russians used the lessons learned from the past and information became one of the major tools for manipulating international public opinion. That opinion had to be won over to the Russian cause by demonizing the enemy, justifying war for a just cause. Those who received the information were certainly not fooled by the possibilities of manipulation that existed then. However, in the context of the global chaos at the time, it was difficult for public opinion to work out what was real from what was false, especially since the questions could not be addressed in such clear-cut terms; that was too simple. True information can be taken out of context, false information can serve a true cause, and information can be partially true and partially erroneous. We also have to consider the moment when information is broadcast, the way in which it is presented, who

broadcasts it, who receives it, how it is duplicated, broadcast, modified and integrated into the environment of global knowledge. From the beginning of the conflict, the Russians carried out psychological operations. Foreign embassies and international organizations received videos showing Chechen cruelty. For the objective of psychological operations and military deception, information must be controlled, whether by traditional media (radio, television) or over the Internet. Strict instructions were imposed on journalists covering the events (the instructions are published on the "infocentr.ru" website, created in 1999 at the start of the conflict). A decree (resolution 1538) from 7 February 2000 reinforced the powers of the Federal Security Bureau (FSB) which can now legally control journalists' access to Chechnya. Psychological operations were combined with electronic warfare operations to intercept communications from the enemy. The Russians were finally able to control the security of radio communications which were the strength of the Chechens in the first war. FAPSI launched a large surveillance operation of radio communications in the North Caucasus called "Experiment 99". The observation satellites launched before the conflict (notably Tselina-2) were vital to this electronic war. They were used during communication interception, location, control, decrypting and disruption operations of Chechen communications. Information warfare extended to the internet, a major vector of psychological operations along with hacker warfare. For psychological operations, both camps used websites to communicate their versions of events and demonize the enemy. This included denunciation of crimes and an escalation of violence in images, the broadcasting of videos of civilian assassinations, the killing of children, torture of prisoners and summary executions. Pro-Chechen sympathizers[125] supported this cause and websites hosted on foreign ground (the qoqaz.net website, for example, based in Malaysia and used as a relay for Chechen propaganda) began to be found. The websites proposed media reports, showed images of victorious operations conducted against Russian troops and interviews with war leaders presented as heroes. Conscious of Russian network war capabilities, pro-Chechen websites had several mirror sites in the

125 kavkaz.org.

world (.com, .my, .de, etc.). The Russians created their own websites and also created confusion by introducing false pro-Chechen sites or pro-Russian sites with domain names very close to the names of Chechen sites. For example, the Russian website kavkaz.com created confusion with the Chechen site kavkaz.org. Psychological operations also used the contribution of interviews with pro-Russian Chechen leaders on antiterror.ru and chechnya.ru. Hacker warfare attempted to paralyze enemy websites. Russian agencies were accused by Chechnya of attacking and paralyzing their kavkaz.org and chechenpress.com websites. After the official end of the conflict, the websites still exist[126], are still active, and support attacks (DoS attacks against servers). When pro-Chechen websites are attacked, they blame the Russian authorities.[127]

In a more general way, and beyond the Chechen question, controlling information circulating in networks is a very significant problem for Russia, which is very sensitive to the possibilities of psychological manipulation of opinion. In 2006, Russia had close to 40 ultranationalist and extremist websites, a quarter of which operated from Russian providers. Ultranationalist sites and very active neo-Nazi sites ("web skinheads") operate freely using the Internet to coordinate their operations, maintain contacts between members throughout the country, and recruit new sympathizers.

3.3.5. *Psychological information warfare*

Control of psychology is a major component in the concept of Russian information warfare [BIL 04]. The objective of information warfare remains the acquisition and control of information, to gain an advantage in terms of information on the enemy. This objective is reached by exerting psychological influence on a government's decision systems, a system that includes decision-makers, all C2 players and the general population (operations of influence, as the Americans would say). This psychological warfare built around psychological operations covers actions such as deception,

126 http://kavkazcenter.com/.
127 http://www.kavkazcenter.com/eng/content/2006/09/27/5731.shtml.

propaganda and misinformation of populations, armies and authorities. The objective is to distort the action phase in the OODA loop by disrupting the observation, orientation and decision phases. In order to do that, the opinions, intentions and decisions of all the players from both sides of a war must be influenced; this includes the enemy and our own camp.

3.3.5.1. *Russia as target of psychological operations*

Even though Russia is developing its offensive psychological warfare capabilities, it must also pay close attention to defensive capabilities. According to studies and reports published in Russia in the last few years, Russian society would be particularly vulnerable to psychological operation attempts launched by enemies.

This vulnerability comes from the cultural, ideological, political and economic shock that disrupted Russian society in the early 1990s, when the Soviet empire collapsed. The balance of the whole social model was in upheaval, starting a period of uncertainty and reassessment, making the population very sensitive to new ideas and to temptations from the West unknown until then. Thus, any information warfare conducted against Russia would attempt to capture this consciousness and undermine the morale of armed forces[128] in order to prepare for a real ideological invasion, to take control of the country's economic and political sectors. If we adopt this point of view, any country that is an ally can be a potential adversary; alliances are no longer possible and there is only one country against the world. The officer proposing this point of view on the dangers of information operations accused psychological warfare activities conducted by countries hostile to Russia of being the cause of all the country's woes. The psychological confrontation therefore becomes the main component of information warfare since it is the vector of the most strategic attacks. Russians call this psychological confrontation "psychological warfare" or "intellectual information warfare".

128 Colonel E.G. Korotchenko, in an article published in the review *La Pensée Militaire* in February 1996.

3.3.5.2. *Components and methods of intellectual warfare*

A permanent psychological confrontation mandates intelligence actions (the collection and analysis of information involving the capabilities of all potential enemies), to predict (from processed data) the nature of psychological operations that enemies or adversaries could conduct, and to evaluate the impact that such psychological operations could have on our own camp. This allows us to adopt active, or even preemptive, defense measures to counter or prevent psychological aggression; to imagine solutions to neutralize the negative consequences of the influence of these psychological operations on the psyche of individuals in times of peace and times of conflict, and to prepare forces (psychological information operations units) to conduct offensive psychological operations in times of crisis and conflict, as well as permanent operations on target populations in times of peace.

The Russian military certainly did not discover psychological operations in 1990 during the Desert Storm campaign! The possibility of manipulating the psyche of enemy troops has long interested Russia's military and its researchers. In fact, mind manipulation is the subject of the conditioned control theory developed by Ivan Pavlov, a 1904 Nobel prize winner. According to him, propaganda produced a subconscious association of ideas, which makes it possible to manipulate minds. What is the impact of psychological operations on the military and on civilians? How can we use information manipulation to affect the reasoning, values, emotions, beliefs, behaviors, decisions and actions of individuals or groups of individuals? How can we efficiently deceive the enemy, distract his judgment, divide, dissuade, suggest and pressure him? How can we affect the enemy's resistance capabilities? All these are objects of study interesting to the Russian military. Russians speak of "maskirovska" to describe deception and misinformation operations aimed at manipulating individual perceptions. We also speak of reflexive control to describe operations to influence decisions by manipulation of information.

Different actions can be launched against the psychological capabilities of individuals in order to affect their judgment, decision process and their behavior:

– Distraction, consisting of creating new real or imaginary threats to force the enemy to re-examine his decisions, change his strategy or tactics, for example reviewing the allocation of resources or repositioning of troops. This operation is intended to force the adversary to make a decision that is detrimental to his camp.

– Overloading is a method consisting of saturating the enemy or adversary with a large volume of contradictory information. The possibilities offered by information systems facilitate overloading. It is possible to create contradictory information and send it through the multiple communication vectors within the information space (Internet websites, e-mail or saturating radars). This possibility shows how difficult it is to provide C2s with necessary, relevant, quality information, at the right time.

– Paralysis consists of selecting the main weaknesses of the target, developing the target's awareness of such weaknesses, and making the target believe that a threat might be able to use such weaknesses.

– Exhaustion consists of multiplying false targets, dispersing the enemy so that he engages in useless operations and launches actions with, if not exhausted, at least depleted resources.

– Deception consists of misleading the enemy to make him take unfavorable decisions, reallocating his forces in the wrong place, for example.

– Division is intended to deceive the enemy into thinking that he must act against the interests of his allies or coalition troops. The objective is to isolate the enemy, make him be the one making a decision which will isolate him irrevocably, so that allied forces eventually have to confront each other, representing an economy of resources for their enemies.

– Pacification is a type of ruse, aimed at making the enemy drop his vigilance through a peaceful attitude. Pacification could take the form of cooperation, or exchanges with "partners" that we consider attacking. Pacification is maintaining that we are implementing

strictly defensive methods, while we know that they can be used offensively. It is the famous argument of "nuclear power with strictly civilian purposes".

– Dissuasion is used to create an impression of superiority. The nuclear bomb is a dissuasion weapon par excellence. In cyberspace, dissuasion could be the threat of network attack capabilities through the use of an impressive arsenal of viruses. It is not as important to be superior as much as it is to give the impression that we are.

– S.A. Komov, the Russian military thinker, adds provocation to this list: leading the enemy to carry out actions unfavorable to themselves. This might consist of offering information affecting the enemy in a legal, moral, ideological or any other way; and of applying pressure, consisting of offering information encouraging society to discredit its own government.

3.3.6. *Players of information warfare*

Information warfare carried out in peacetime and in wartime involves the players responsible for security and national defense including intelligence agencies and the army. But it also involves hackers.

3.3.6.1. *Government agencies*

Following the failed coup against Mikhail Gorbachev, the KGB (Committee for State Security) was dismantled in 1991 into several independent security departments, one of which was the Federal Agency for Government Communications and Information (FAPSI).

This agency was the equivalent of the American NSA and its missions were to ensure the security of the State's encrypted communications, the protection of the government's websites against hacking and electronic intelligence (interception of encrypted communications and cryptanalysis) from its three centers spread over the Russian territory. From 1995, it had control over cryptography systems and was the only agency with the authority to grant licenses. More globally, it was responsible for all encrypted communications. It often unsuccessfully tried to gain control of the Internet.

During its operation, it collected, processed and stored large volumes of data in all sectors of social activity: political, economic, legal, financial and industrial. These resources were distributed between the Federal Security Bureau (FSB) and Defense Ministry after FAPSI was dismantled in March 2003.

The FSB is Russia's secret police, born out of the ex-KGB. It inherited from FAPSI all activities involving telephone communications, mobile telephony, Internet, government secure communications, control of the system of electronic transmissions of election results (the "Vybory" system) and cryptography and encryption activities.

The FSB is considered to be the second most important army formation outside of the military itself.

3.3.6.2. *The military*

For Russia, the Desert Storm campaign was the confirmation of their predictions of the growing power of the American military, and of the capabilities now available to the military that chooses transformation by the introduction of information and communication technologies. That campaign paved the way for a new era, the era of wars based on information control. The Russian army also had to focus its efforts and reflection on the capabilities of information warfare, knowing that it did not have the same (financial) resources as the United States, especially since the country was not in a favorable period for investing in the military sector[129].

The war in Kosovo (1999) was perceived as the first contactless war, a virtual war during which superiority of information benefiting NATO ensured victory. Russia was not able to compete with the United States or with NATO forces. Because it was in a situation of technological inferiority, it could only rely on the asymmetrical option, notably asymmetrical information warfare. Solutions needed to be developed to affect the Achilles heel of greater military powers, disrupting the enemy's OODA cycle.

---

129 See M.C. Fitzgerald, "Russian views on electronic signals and information warfare", *American Intelligence Journal*, Signals Intelligence & Information War, Spring/Summer 1994 (vol. 15, no. 1), USA.

Modernization of armies is based on the creation of an integrated information environment, a single military standards system to transmit data. In January 2000, President Putin announced that from now on Russia had to increase the development of new high-tech weapons.

Is Russia very behind in terms of information warfare capabilities, by comparison with the West? That is not the conclusion of a report from the American Defense Science Board[130] which says that, on the contrary, Russia's information warfare capabilities are very high and include defensive cyberwar capabilities, development of software weapons (viruses able to break through IS security, to propagate and to defend themselves; reprogrammable memory chips, Trojan horses and remote attack tools), the development of electronic warfare capabilities (radars, jamming devices and espionage), hacking to steal information, development of guided weapons and electromagnetic power (EMP) anti-satellite weapons, more precise modern satellites, navigation equipment for soldiers, reconnaissance systems, automated air force control systems and C2 systems for nuclear strategic forces. The list is not complete but Russia is working on the development of specific methods for each component of information warfare.

3.3.6.3. *Hackers*

There are not many certainties in this field. The idea that a government can attack another government and that this aggressor uses hackers is based on assumptions, or even allegations.

Whether these hackers are part of the armed forces or of the secret services, or whether they are paid "by the task", is irrelevant in the end. What is important is the threat, the aggression and the aggressor. Recently, the finger was pointed at Russia by the international community, not only because the whole planet sustained attacks from its spammers and other cyber delinquents for financial gain, but also for its "espionage campaigns" conducted against sensitive websites, as denounced by the United States. In February 1998, the Solar Sunrise affair emerged. Hackers penetrated the networks of the American

130 www.acq.osd.mil/dsb/reports.htm.

Department of Defense. The guilty party named was Russia. An investigation revealed that, in fact, it was two American teenagers living in California! In 2000, the Americans discovered that a wide espionage campaign begun in 1998 (and called "Moonlight Maze") affected 2 million computers in the United States. The Pentagon, NASA, the Energy Department, private universities and research laboratories, private American cryptography tools development companies, and the command center of space and naval war systems (Spawar) in San Diego were some of the victims. After investigation, Russia and the Moscow Science Academy were accused of involvement. But who were the sponsors? Was the Russian government involved? If so, at which level? The main characteristic of these network attacks is that it is extremely difficult to get to the real source of the aggression.

3.3.7. *Hybrid warfare and information warfare*

There have been a number of definitions put forward for hybrid warfare:

– "sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion"[131];

– "a blend of the lethality of state conflict with the fanatical and protracted fervor of irregular war"[132];

– "the use of different forms of conventional and non-conventional warfare tactics at the same time"[133];

– "a hybrid threat is one posed by any current or potential adversary, including state, non-state and terrorists, with the ability, whether demonstrated or likely, to simultaneously employ

131 Military Balance 2015, International Institute for Strategic Studies.

132 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington, VA: Potomac Institute for Policy Studies, 2007.

133 Robert Seely, "Russia's New Warfare tools and the link to Soviet Active Measures", *Georgian Review*, p. 15, 2015, http://georgianreview.ge/wp-content/uploads/2015/09/bob-pdf.pdf.

conventional and non-conventional means adaptively, in pursuit of their objectives"[134];

– "hybrid warfare is a conflict executed by either state and/or non-state threats that employs multiple modes of warfare to include conventional capabilities, irregular tactics, and criminal disorder"[135];

From these definitions, it seems that hybrid wars did not emerge with Russia's intervention in Crimea. The expression was also used in 2005 to denote Hezbollah's tactics against Israel. This modern Russian hybrid war is rooted in the Soviet period[136]. There are opposing opinions as to the innovativeness of Russian information warfare and of its manner of waging hybrid war[137]. Whatever the point of view adopted, hybrid wars have, like all modern forms of conflict, integrated new technologies, and therefore undergone a number of transformations. Thus, it is worth looking carefully at the changes induced by the technologies, and more specifically information technologies:

– the lack of consensus, agreements, international convergence as to the way of dealing with cyberthreats and threats in information space, as to the way to defend and secure these spaces, give rise to fragility – vulnerabilities which Russia was keen to exploit in its conflict with Ukraine, as it did in Georgia in 2008. The situation in Crimea will only have increased that fragility of the international community in relation to the information sphere;[138]

---

134 NATO Military Working Group, Strategic Planning & Concepts, 2010.

135 Andis Kudors, Hybrid War – A New Security Challenge for Europe, Background notes, Latvian presidency of the council of the European Union, June 2015, http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf.

136 Maria Snegovaya, Putin's Information Warfare in Russia. Soviet origins of Russia's Hybrid Warfare, Russia Report 1, Institute for the Study of War, Washington DC., p. 28, September 2015.

137 Robert Seely, "Russia's New Warfare tools and the link to Soviet Active Measures", *Georgian Review*, p. 15, 2015.

P. Pomerantsev, "How Putin Is Reinventing Warfare", *Foreign Policy*, 2014: http://www.foreignpolicy.com/articles/2014/05/05/how_putin_is_reinventing_warfare.

138 Eve Hunter, Piret Pernik, The Challenges of Hybrid Warfare, International Centre for Defence and Security, Tallinn, Estonia, April 2015, http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf.

– the international community has not managed to reach an agreement as to what constitutes an act of war in the information sphere: does an intrusion into a computer system qualify as one? The states themselves do not always have a clearly-defined judicial, political and strategic stance on the issue. The lack of definition constitutes a weakness, but it can also be useful for states, who can therefore play on the imprecise legal boundaries;

– information warfare occupies a central place in hybrid war: intrusions into foreign social media, into systems; viral attacks (following the example of the malware BlackEnergy which targeted Ukrainian governmental organizations); psychological operations (disinformation, influence, targeting national and international public opinion by creating media, occupying the media space, maintaining a strong presence on social networks, employing strategies of influence on social media; making an effort to control and limit any expression of a dissident voice); attacks on C2 (Command and Control) systems (e.g. paralyzing the enemy's logistical systems, the communication systems of the leaders and the military decision-makers). Here we find the conventional elements of information operations in times of conflict – the elements of information warfare defined 20 years earlier;

– Russian information warfare seems to be centered on psychological operations, and particularly on reflexive control[139], which was developed during the Soviet period;

– in terms of cyber, the aggressors hide behind the principle of non-attribution to refute the accusations. They can also reject responsibility for aggressive operations against patriotic hackers, or opportunistic cybercriminals, whom the government are unable to control;

– the arguments available to states (it is difficult or impossible to assign blame; the actors cannot be controlled) to deny their

139 Maria Snegovaya, Putin's Information Warfare in Russia. Soviet origins of Russia's Hybrid Warfare, Russia Report 1, Institute for the Study of War, Washington DC., September 2015.

responsibilities (cyber attacks) create a line of defense in their favor – a screen to mask their true activities.

The novelty of hybrid war, at least for that contained in the information warfare dimension thereof, of course lies in the expansion of the social networks. This expansion opens up a perimeter of international influence never before seen, but also renders the task of controlling the information space much more difficult, and informational dominance *a priori* more difficult to achieve. The more the information spectrum expands, the more, potentially, the adversaries/enemies' range of action expands too.

Type of operation	Objective
Deception operations	Example: masking the presence of Russian troops in Ukraine
Masking one's intentions	Making certain people afraid, and convincing others that Moscow's objectives are limited or acceptable
Denying Russia's involvement in the conflict	Not appearing to be a belligerent state on the international scene
In parallel, threatening the West (flyovers of member states of NATO, intrusion into national airspaces)	Convincing people of Russia's military power
Making a significant effort to dominate the narrative, particularly in social media	Creating history, influencing, dominating the information sphere

Table 3.5. *Techniques of reflexive control, according to Maria Snegovaya, 2015*[140]

It is also defined thus:

– the center of gravity to be targeted is the enemy population;

– the attack on Ukraine by Russia in 2014 demonstrates the importance of information warfare in these new-generation conflicts;

140 Maria Snegovaya, Putin's Information Warfare in Russia. Soviet origins of Russia's Hybrid Warfare, Russia Report 1, Institute for the Study of War, Washington DC., September 2015.

– military engagements in all dimensions simultaneously (land, air, sea, information);

– the purpose of hybrid war is to destabilize a state even before it realizes that a war has begun;

– cyber attacks are only one component of this form of war.

Various definitions of hybrid warfare exist. For example, one definition is that "hybrid warfare is a conflict executed by either state and/or non-state threats that employs multiple modes of warfare to include conventional capabilities, irregular tactics, and criminal disorder". In 2010, the NATO Military Working Group (Strategic Planning & Concepts) approved the following definition: "A hybrid threat is one posed by any current or potential adversary, including state, non-state and terrorists, with the ability, whether demonstrated or likely, to simultaneously employ conventional and non-conventional means adaptively, in pursuit of their objectives".

3.3.8. *Information warfare: what is new…*

In many aspects, though, information warfare as described and laid at Russia's door seems to be relatively conventional in its foundations. In particular, it is very typical to hold the conviction that a war can be won or avoided by non-violent means[141], in which information warfare plays a part: "the "role of non-military means to achieve political and strategic aims has increased, which in some cases far exceeds force of arms in its effectiveness" (remarks attributed to General Gerasimov, 2013)[142].

141 Jolanta Darczewska, "The devil is in the details. Information warfare in the light of Russia's military doctrine", *Point of View*, Center for Eastern Studies, Warsaw, no.50, p. 39, May 2015, , http://www.osw.waw.pl/sites/default/files/pw_50_ang_the-devil-is-in_net.pdf.

142 V. Gerasimov, V., Tsennost Nauki v Prdevidenii, Voenno-Promishlennyii Kurier, p. 2, 27 February to 5 March, 2013, http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf, cited in Robert Seely, "Russia's New Warfare tools and the link to Soviet Active Measures", *Georgian Review*, 15 pages 2015.

However, numerous authors – particularly in view of the observation of the conflict with Ukraine in 2014-2015 – affirm that Russia symbolizes the renewal of the importance of information warfare in armed conflicts.

Thus, here, let us focus on identifying the markers of this "novelty" in Russian doctrine, thinking and practice in terms of information warfare. In order to do so, let us make a number of comparisons. In 1996, Timothy L. Thomas wrote about Russian information warfare[143]. In 2010, he published an article on the subject[144], based on the study of the Russian-Georgian conflict. In May 2014, Jolanta Darczewska published a study on Russian information warfare, based on an analysis of the situation in Crimea[145]. Might it be possible, by comparing these three reflections, to reveal the evolutions which have taken place in recent years?

Thus, from Timothy L. Thomas' 1996 analysis on Russian information warfare, we find that:

– information warfare is defined by the Russians themselves as:

- a way of resolving conflicts,

- a set of practices whose purpose is to acquire the informational advantage over adverse part,

- a set of practices targeting the decision-making systems of the enemy nation, its population, and its informational structures and resources,

- psychological and technical actions of influence,

143 Timothy L. Thomas, "Russian views on information-based warfare", *Airpower Journal*, USA, pp. 25-35, 1996, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj96/spec96/thomas.pdf.

144 Timothy L. Thomas, Russian Information Warfare Theory. The consequences of August 2008, Strategic Studies Institute of the US Army War College, United States, July 2010.

145 Jolanta Darczewska, "The anatomy of Russian information warfare. The Crimean operation, a case study", *Point of View*, Poland, no. 42, p. 37, May 2014, http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.

- operations which, in order to achieve their objectives, can make use of additional means such as nuclear weapons, electronic weapons, etc.;

– the use, in the field of military operations, of intelligence, C2, communication, deception, electronic warfare resources, to support the action of the forces;

– the FAPSI (Federal Agency for Government Communications and Information) plays the role of defender against information weapons;

– malware serves as weapons;

– the information component is important in evaluating the combat potential;

– psychological operations occupy a central place (perception management, manipulation of information, reflexive control, mobilization of mass media).

According to Timothy L. Thomas (2010), Russian IW was characterized thus:

– firstly, the Russia-Georgian conflict is considered to be a key moment, because it seems to have conditioned the renewal of Russian theoretical, strategic and military capacity renewal in terms of information warfare:

- confirmation of the importance of IW for the Russian leaders, during summer 2008 (Russian-Georgian conflict),

- Russia became awareness of the weaknesses and failures at capacity- and theoretical level in terms of information,

- Russian experts concluded that Russia lost the information war in the Russia-Georgian conflict and that Russia's geopolitical and geo-economic place would be directly determined by its capacity to use information warfare (and thus first of all to create the means to wage such a war);

– however, there is a new dynamic, rather than a novelty, because for a long time, Russia has been including that informational dimension in its strategy, whether political or military:

- at a political level, Russia is taking pains to create an information environment which serves its interests on the international scene (definition of international strategies, participation in international forums concerning the Information Society (for example, the World Summit on Information Societies), and weaving a national framework by legislating (e.g. the fight against cyber crime; publication of the Information Security Doctrine of the Russian Federation in 2000; "Strategy on information society development in Russia" in 2008; and "National Security Strategy" in 2009). Information security is crucially important. It is not just a question of cybersecurity; the focus is placed clearly on information. Information security was defined in 2000 as "the state of protection of its national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state". In the military field, information security pertains to the information infrastructure (notably at the level of C2), the information resources of defense companies; software and hardware of C2 systems. Informational threats against the army notably include psychological ones which can affect the soldiers themselves (destabilization, psychological operations intended to undermine their morale, their patriotism) and foreign espionage operations,

- at a military level, ICT occupies a major place in both theory and doctrine, and the main focus is on two aspects of information warfare: its technical component and its psychological component,

- at the national or international levels, political and military, Russia's leaders are devoting specific attention to the power of information and influence, having experienced the failure of an ideology (the end of the Cold War). In order to avoid history repeating itself, with an adverse ideology ousting a regime, Russia is developing domestic doctrines and policies of information security (ensuring the psychological stability of the general population, but also of the soldiers). The information sphere is the vector of a threat to national security, and this has been being stated since the 1990s. This view of security is based on the observation of development of strategies, doctrines, capabilities and practices by numerous states throughout the world, whose efforts could be turned against Russia.

Information warfare threats are at once external and internal. Thus, it is wise to fight on all fronts at once;

– Russia is painting itself as the target of constant attacks or threats of information attacks by foreign powers. This stance as a victim helps to legitimize its policies. The purpose is to counter the informational attacks targeted at Russia. In the line of fire, naturally, are the United States, NATO and the West in general. Russia regularly complains of psychological warfare operations carried out by NATO in the support it provides to Russia's neighbors[146];

– the counter-measures envisaged to counter foreign attacks employ a broad range of means and methods: counter-propaganda, use of the media, identification of enemy information sources, electronic warfare, psychological warfare, hacking, etc. (information warfare of course involves the Net).

Russian information warfare as described by Jolanta Darczewska in light of the conflict with Crimea would be characterized thus:

– Russian information warfare has developed as a response to the Western concepts of next-generation warfare;

– when information war is waged against Russia, it can respond with conventional war;

– Russian information warfare is built on two pillars: psychological warfare, inherited from the Soviet era; and today's technological pillar;

– in geopolitical doctrine, information is considered as a weapon: cheap, universal, limitless, easily accessible, and capable of striking across any border;

– Russia uses netwar and information warfare and psychological warfare to achieve its national, international and regional objectives;

146 Plans of Ukraine-NATO psychological warfare against Russia appear online, Pravda,10 April 2015: http://english.pravda.ru/russia/politics/10-04-2015/130248-nato_psychological_warfare-0/#sthash.PZUcASWP.dpuf.

– the influence of a few key geopolitical figures is central in the formulation of the role of information- and psychological warfare. Two figures in particular can be distinguished:

- Igor Panarin (professor at the Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation), who in 1995 laid down the foundations of an information-security doctrine. Panarin states that the color revolutions and the Arab Spring movements are the result of American informational aggression. According to him, the essential building blocks in information warfare are: social control, social maneuvering, information manipulation, disinformation, fabrication of information, lobbying, blackmail, extortion of desired information). He distinguishes between two types of information warfare: informational-technical and informational-psychological. In the former, the targets are technical (systems, means of communication, etc.); in the latter they are human, decision-making[147],

- Alexandre Dugin, who introduced the concepts of netwar and Net-centric warfare in Russia, using the examples of the color revolutions, and proposed a model of Eurasian netwar. This netwar must be capable of offering a symmetrical response to the netwar conducted by the United States. This netwar must be based on a network of actors mobilizing intelligence agencies, intellectuals, scientists, journalists and activists. However, it is a prerequisite for the success of the project that these actors be "postmodernized";

– this geopolitics offers a theoretical/ideological framework for Russia's action and policy, by promoting a neo-Conservative post-liberal power, whose aim is to create a just and multipolar world, defending traditions, conservative values, freedom, Eurasian-Russian civilization. This stance brings Russia into conflict with the America-centric Western world. The Crimea crisis is the expression of this rivalry between two models of civilizations. This world view has been outlawed since the end of the Cold War. The information strategy associated with that objective is constructed around defense and reinforcement of the state, and of its social, scientific, media, diplomatic (etc.) bases. Internally, the goal is to mobilize the

147 Jolanta Darczewska, The anatomy of Russian information warfare. The Crimean operation, a case study, Point of View, Poland, no. 42, p. 37, May 2014.

population. Externally, the aim is to reconstruct Russia's sphere of influence;

– the strategy of information/psychological warfare, therefore, is a question of survival of civilization, the fight against the informational aggression of Atlantic civilization carried out by the United States. The struggle against terrorism does not seem to be the main legitimizing force behind the political and strategic choices;

– this theoretical/ideological geopolitical background nature offers us a lens through which to view and interpret the strategies and practices of Russian information warfare;

– Western public opinion seems to be fairly resistant to Russian propaganda. However, Russian propaganda is likely to intensify, and gain the most modern of influence vectors;

– the strategy consists of mobilizing a very broad range of actors in the deed – e.g. the campaign of disinformation conducted in the Ukrainian conflict. Indeed, this disinformation campaign involved diplomats, politicians, experts, academic researchers and members of the cultural elites. Disinformation is also combined with other practices: provocation, diplomatic activity, etc. Ultimately, the operations take place over a period of time (several years).

4

Concepts and Theories: Discussions

4.1. Doctrines

Today, there are two categories of sources which share the definition of the concepts, notions and policies of security: firstly the military doctrines, and secondly the strategies formulated by civil State-run institutions, national and international institutions and organizations. We could also add company strategies, which sometimes take the form of "white papers", expressing visions of the cybersecurity environment, the observations, produce analyses, put forward solutions, or even propose their own definitions of concepts such as cyber crime, cyberthreat, cybersecurity, cyberspace, etc. Here, though, we shall focus mainly on State sources.

Throughout the previous chapters, we have based our discussions on the defense doctrines. It is worth lingering over the role of doctrine, generally, and asking about the pertinence of that source, as a basis for understanding not only a state's thinking about security issues, but also as the foundation of security practices.

The functions which we can attribute to doctrine are many:

– in a comparative analysis, for example, it helps to show the dynamic, evolutive and adaptive nature (e.g. by distinguishing those which have and have not integrated the cyber technological transition; or those which have altered in view of the evolution of the

Information Warfare, First Edition. Daniel Ventre.
© ISTE Ltd 2016. Published by ISTE Ltd and John Wiley & Sons, Inc.

international political context[1]) of a military school of thought, a state[2], or else to underline the conservative and rigid nature (such as the judgment made by American experts about Russia's military doctrine published in 2015. "Russia's New Military Doctrine: Same as the Old Doctrine, Mostly"[3]);

– military doctrine is an important component in national security policy, but it is not the only one;

– doctrine is a reflection, which can help steer the security policies;

– the formulation of a doctrine may reveal internal competition within the military institution, of movements under way, of a reorganization;

– it may express the convergence of a school of thought with another state's way of thinking, its allegiance strategies (e.g. when a doctrine offers conceptual definitions that are close to those of the organization to which the state belongs – an example can be found in the definitions adopted by the member states of NATO).

However, the doctrine does not always mean:

– that the practice actually corresponds to the thinking formulated therein;

– that its publication will product immediate or even long-term effects on the organization and military strategy;

– that the military, conceptual and strategic thinking expressed is specific to one state in particular;

– that the concepts employed are all precisely defined.

---

1 Mansoor Jafar, "Pakistan's new military doctrine under Indian threats", *Al Arabiya News*, 8 January 2013, http://english.alarabiya.net/views/2013/01/08/259256.html.
2 M.V. Rappai, "Changes in Chinese Military Doctrine and their implications", *Strategic Analysis*, vol. 23, no. 4, pp. 615–626, 1999.
3 Olga Oliker, "Russia's New Military Doctrine: Same as the Old Doctrine, Mostly", *TheRandBlog*, January 2015, http://www.rand.org/blog/2015/01/russias-new-military-doctrine-same-as-the-old-doctrine.html.

The primary function of doctrine – particularly since the advent of the Internet and the resulting availability of access to official sites – is to help a state construct the image of itself which it wishes to project to the international community. Note also that a number of non-English speaking countries have their doctrines translated into English, so as to render them more accessible and reach a wider audience. Doctrine can be considered to be a tool for communication and for influence in the arena of international politics.

In awareness of these characteristics of doctrine, it is used in this chapter to try to demonstrate the conceptual and theoretical evolutions, regarding information and cyber in military thinking.

Country	Title	Date	Concepts not used	Concepts used
Australia	Australian Maritime Doctrine[4]	2010	– cyberspace – cyber operations – information warfare	– data – information operations – information environment
Australia	Foundations of Australian Military Doctrine ADDP–D[5]	May 2012	– cyberspace operations – cyberspace – information warfare – data	– information operations – information[6]
Canada	Canadian Forces Joint Publication. CFJP 01. Canadian Military Doctrine[7]	April 2009	– information environment – information warfare – information operations	– data – information technologies/ systems/ networks/ structures

4 https://www.navy.gov.au/sites/default/files/documents/Amd2010.pdf.
5 http://www.defence.gov.au/adfwc/Documents/DoctrineLibrary/ADDP/ADDP-D-FoundationsofAustralianMilitaryDoctrine.pdf.
6 "There are four physical domains: maritime (including sub-surface), land, air and space. The two non-physical domains are information (including cyber and the electromagnetic spectrum) and the human domain".
7 http://publications.gc.ca/collections/collection_2010/forces/D2-252-2009-eng.pdf.

			– cyber – cyberwar – cyberspace	
Canada	Canadian Forces Aerospace Sense Doctrine[8]. B–GA–402–000/FP–001 Commander of the Royal Canadian Air Force	August 2012	– information warfare – information environment/ sphere/space – information operation	– data[9] – cyberspace – information superiority
France	Doctrine of the employment of the French armed forces. Joint doctrine. (FRA) JD–01(A)_DEF(2014) No. 128/DEF/CICDE/ NP[10]	June 2014	– information warfare – cyberspace operations	– information environment – information operations – cyberspace – data
Ireland	Green paper on defence[11]	July 2013	– cyberspace – information environment/ space/domain – information operation – information warfare	– data – cyber – information
Lithuania	Lithuanian Military Doctrine[12]	2010	– cyber operations	– information

8 http://airforceapp.forces.gc.ca/cfawc/CDD/Doctrine/Pubs/Operational/402_Series/B-GA-402-000-FP-001.pdf

9 The formula “data and information” recurs frequently. This highlights the distinction that must be drawn between the two notions. Throughout the document’s 56 pages, the term “data” is used 108 times, which attests to the importance attached to the object (“information” is mentioned 268 times, but “cyber” only three times). We shall use this document for observation of military treatment of data, alongside their treatment of information and cyber.

10 http://www.cicde.defense.gouv.fr/IMG/pdf/20140612_np_cicde_fra-jd-01a-def.pdf.

11 http://www.nuigalway.ie/media/staffsub-sites/researchoffice/images/Green-Paper-of-Defence.pdf.

			– cyberspace operations – information warfare – data	– information environment[13] – cyber – information operations – cyberspace[14]
NATO	NATO standard AJP–3.4.9. Allied Joint Doctrine for Civil–Military Cooperation (CIMIC)[15]	February 2013	– information warfare – cyberspace – cyber operations Cyberspace operations	– information operations – information environment – data
Netherlands	Netherlands defense doctrine[16]	November 2013	– information warfare – cyberspace operations – information environment	– cyber warfare (CNO) – cyber operations – information operations – information domain[17] – information activities – data

12 http://kariuomene.kam.lt/download/19294/lithuanian%20military%20doctrine-2010.pdf.

13 “Information environment is assessed in the following three aspects: physical aspect [...], information aspect [...], cognitive aspect”.

14 “Information aspect also includes the cyberspace”.

15 http://www.cimic-coe.org/wp-content/uploads/2014/06/AJP-3.4.9-EDA-V1-E1.pdf.

16 https://www.defensie.nl/binaries/defensie/documenten/publicaties/2013/11/20/defence-doctrine-en/defensie-doctrine_en.pdf.

17 “This domain encompasses all forms of storage and transfer of information, regardless of the form it takes (oral, on paper, via radio and television, internet or other electronic or non-electronic means). Although the information domain is often dependent on physical means in the other domains (transmitters, satellites, servers), it is in principle largely unaffected by the boundaries that apply in the other domains. The dimension referred to as cyberspace forms part of the information domain and comprises the storage and transfer of information by digital media”. “The information domain is regarded as a public domain which cannot be captured but in which temporary and local information superiority can be achieved”.

New Zealand	New Zealand Defense Doctrine – NZDDP–D[18]	June 2012	– information operations – cyberspace operations – cyber operations – data	– information warfare[19] – information environment – cyberspace – data
Norway	Capable Forces. Strategic Concept for the Norwegian Armed Forces[20]	2009	– information domain/ environment/ space – information operations/ activities – cyberspace – data	– information
UK	UK Air and Space doctrine. Joint Doctrine Publication 0–30 (JDP 0–30) directed by the Joint Forces Commander and Chiefs of Staff[21]	July 2013	– information environment – cyberspace operations	– cyber operations[22] – information operations[23] – data
UK	Joint Doctrine Note 2/13. Information Superiority[24]	August 2013		– data – information environment – information operations – information

18 http://www.nzdf.mil.nz/downloads/pdf/public-docs/2012/nzddp_d_3rd_ed.pdf.
19 "Corrupting or disabling key information databases and systems".
20 https://www.regjeringen.no/globalassets/upload/fd/dokumenter/capable-force_strategic-concept.pdf.
21 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/223495/jdp_0_30_uk_air_and_space_doctrine.pdf.
22 "Cyber operations are a related activity that creates military effects across cyberspace. An adversary's dependence on digital networked systems determines their offensive potential".
23 "Information operations are a staff function which analyses, plans, assesses and integrates information activities".
24 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/239342/20130813_JDN_2_13_Info_Super.pdf.

				warfare – cyberspace – cyber operations
UK	Cyber Primer. Joint Force Commander and Chiefs of Staff[25]	December 2013	– information warfare	– cyberspace[26] – cyberspace operations[27] – information environment[28] – information operations – data
UK	Joint Doctrine Publication 0–01 UK Defence Doctrine[29]	November 2014	– cyberspace operations – information operations	– cyberspace[30] – information environment[31] – data
UK	Army Doctrine Publication. Operations[32]	December 2010	– cyberspace operations – information operations – information	– cyberspace – information environment – information[33] – data

25 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf.
26 "Cyberspace is the interdependent network of information technology infrastructures, (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein within the information environment. (JDN 3/13)".
27 "The employment of capabilities where the primary purpose is to achieve effects in, or through, cyberspace. (JDN 3/13)".
28 Concept not defined in this document.
29 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf.
30 "Cyberspace is an operating environment within the information environment".
31 Concept not defined in this document.
32 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/33695/ADPOperationsDec10.pdf.
33 Information consists of unprocessed items, series or groups of data, which are collected by sensors or sources and then interpreted and placed in context, in order to expose meaning, accuracy and reliability. Information is only of value if shared, within a secure system.

			warfare	
USA	JP 3–22. Foreign Internal Defense[34]	12 July 2010	– information warfare – cyberspace – cyberspace operations – cyber operations – cyber warfare	– Information operations – information environment – data
USA	ADRP 1–02, Operational Terms and Military Symbols[35]	August 2012, modified 28 November 2012	– information operations – cyberspace – cyber operations	– information environment – information[36] – data[37] – cyber
USA	ADP 3–90 Offense and Defense[38]	August 2012	– information warfare – information environment – information space/sphere – cyber – cyberspace – cyber warfare – data	
USA	Joint Publication 1 – Doctrine of the Armed Forces of the United States[39]	25 March 2013	– information warfare	– information operations – information environment – data

34 http://www.dtic.mil/doctrine/new_pubs/jp3_22.pdf.
35 http://armyrotc.msu.edu/resources/adrp1_02.pdf.
36 "The meaning that a human assigns to data by means of the known conventions used in their representation (ADRP 1-02)".
37 "(Army) Unprocessed signals communicated between any nodes in an information system, or sensing from the environment detected by a collector of any kind (human, mechanical, or electronic) (ADRP 6-0)".
38 Army Doctrine Publication, Department of the Army Washington, DC, p. 32, 31 August 2012, http://www.benning.army.mil/mssp/PDF/adp3_90.pdf.
39 http://www.dtic.mil/doctrine/new_pubs/jp1.pdf.

				– cyberspace – cyberspace operations
USA	FM 3–38; CEMA Cyber Electromagnetic Activities[40]	February 2014	– information warfare	– information operations – information environment – cyberspace[41] – cyberspace operations – data
USA	Department of Defense Law of War Manual[42]	June 2015	– cyber warfare – cyberwar – information, warfare	– cyber operations – cyberspace – information operations – information environment – data
USA	ATP 3–05.2, Foreign Internal Defense, Department of the Army[43]	August 2015	– information warfare – cyberspace – cyberspace operations – cyber warfare	– information environment – information operation – data

Table 4.1. *Military Doctrines 2010–2015[44]. Some examples of uses of notions associated with "data", "information" and "cyber"*

40 http://fas.org/irp/doddir/army/fm3-38.pdf. In the proposed approach, defining the relations between the different domains, cyberspace and the electromagnetic spectrum are both defined as being elements of the information space.

41 "Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 1-02)".

42 http://www.dod.mil/dodgc/images/law_war_manual15.pdf.

43 http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/atp3_05x2.pdf.

44 Table compiled by collecting the Google responsible for a search for "armed forces doctrine".

	Australia	Canada	France	Ireland	Lithuania	NATO	Netherlands	New Zealand	Norway	UK	USA
Information environment/ domain/space/sphere	✓		✓		✓	✓	✓	✓		✓	✓
Information operations	✓		✓		✓	✓	✓			✓	✓
Information warfare								✓		✓	
Cyberspace		✓	✓		✓			✓		✓	✓
Cyber operations							✓			✓	✓
Cyber warfare							✓				
Data	✓	✓	✓	✓		✓	✓			✓	✓

Table 4.2. *Main concepts in a number of military doctrines (2009–2015)*

From the above two tables, we can take away that the concept of information warfare is actually practically disappearing from doctrinal vocabulary, and that the expression "cyber warfare" is not any more widely used. Three subsets can be shown to exist: that of information, that of cyber, and that of data.

4.2. Information warfare: definitions, models

Our aim is to define and then attempt to model the objects in question, in order to then be able to imagine and model the conflicts

which take place. However, at this stage, we shall not speak of representations or of cartography.

Various concepts have been mentioned in this book. To begin with, let us look at the information environment (or information sphere, domain or space). Around information, we consider there to be a whole set of infrastructures, actors, actions, which/who construct information, share it, process it and exploit it. This set is called an environment. We shall then look again at the concept of "information warfare", its definitions and its models.

4.2.1. *The information environment*

The information space (also known as the information environment, information sphere), invites a number of definitions.

Source	*Definition*	*Date*
Robert Cordray, Marc J. Romanych[45]	"The information environment is a construct based upon the idea that the existence and proliferation of information and information systems creates a distinct operating dimension or environment. As a combination of tangible (physical information systems and networks) and intangible elements (information and decision-making), the information environment is both a resource for military operations and a medium in which armed forces operate".	2005
Arto Hirvela[46]	"The information environment is as abstract as information itself […] The information environment consists of information, information structures, individuals, systems, and organizations that collect, process, store, share and present information".	2006

45 Robert Cordray, Marc J. Romanych, "Mapping the Information Environment, IO Sphere", available at: http://www.au.af.mil/info-ops/iosphere/iosphere_summer05_cordray.pdf, USA, pp. 7–10, 2005.

46 Arto Hirvela, "Discovering how information warfare distorts the information environment", *Proceedings of the 5th European Conference on i-Warfare and Security*, pp. 71–80, 2006.

Inta Brikše[47]	"The information environment, which is often associated with the issue of information ecology, represents a set of factors, resources, and processes, which demonstrate the knowledge that has been accumulated and used by a specific society, community or individual, looking also at ideas and assumptions".	2006
U.S. Joint Chiefs of Staff. JP –3–13 Information Operations[48]	"The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive".	2014

Table 4.3. *Definitions of the "information environment"*

This information space is not unified, unique or global. It is made up of a multitude of subspaces, subsystems and subnetworks. The sharing of these spaces, their interrelation, their overall approach, has been the subject of numerous discourses employing the concept of the Joint Information Environment (JIE)[49] and the Information Sharing Environment (ISE).[50]

47 Inta Brikše, "The information environment: theoretical approaches and explanations", in *Informācijas vide Latvijā: 21. gadsimta sākums*, *Rīga*, 2006, available at: http://www.szf.lu.lv/fileadmin/user_upload/szf_faili/Petnieciba/sppi/mediji/inta-brikse_anglu.pdf.

48 Joint Chiefs of Staff, Information Operations, JP 3-13, available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, 27 November 2012 Incorporating Change 1 20 November 2014.

49 Lisa Ferdinando, "Joint Information Environment is 'operational imperative'", U.S. Army, available at: http://www.army.mil/article/152064/Joint_information_environment_is__operational_imperative_/, 2015.

50 Office of the Director of National Intelligence, Information Sharing Environment Implementation Plan, Washington D.C., p. 186, November 2006, http://fas.org/irp/agency/ise/plan1106.pdf.

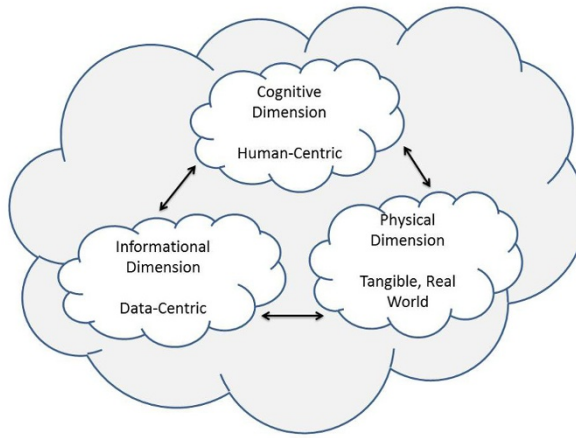


Figure 4.1. *Information space as defined in JP 3–13*

Cyberspace – the technical foundation upon which modern society largely rests – occupies an increasingly large place in that information space[51], even though it is still only a subset thereof. If we look again at the simplified model of the information environment with 3 layers, strata, levels, the representations of cyberspace can quite easily be derived from it. Cyberspace adopts the same structure as information space.

What is cyberspace?

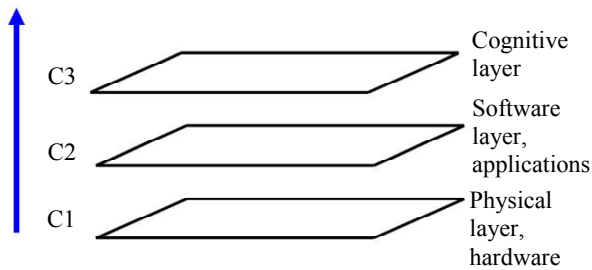


Figure 4.2. *Three layers of cyberspace*

51 Isaac R. Porche III, *et al.*, "Redefining Information Warfare Boundaries for an army in a wireless world", Rand Corporation, United States, 2013.

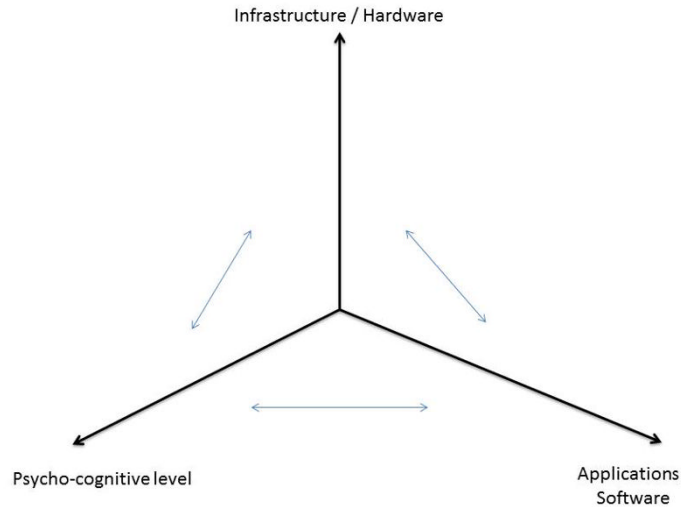


Figure 4.3. *Cyberspace in the form of a three-dimensional system*

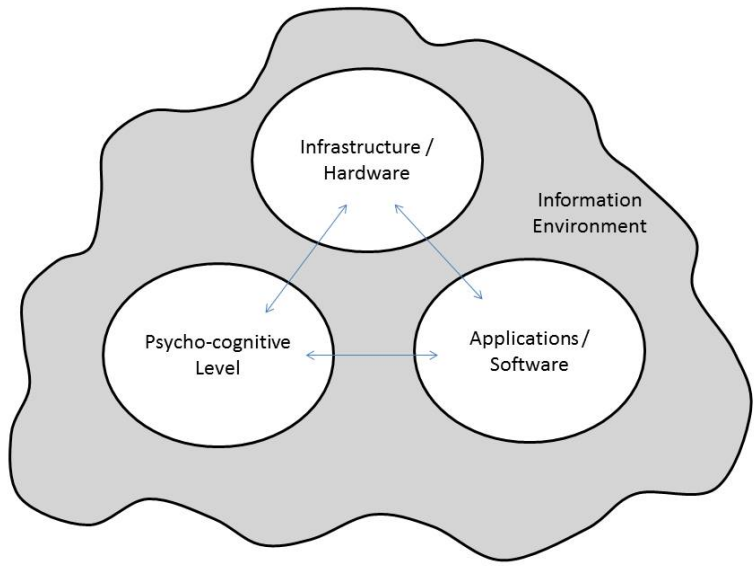


Figure 4.4. *The three components of cyberspace, as they fit in to the information environment*

If we accept this formulation, where cyberspace is a component of information space – which, for its part is far more extensive – we find ourselves with two domains with very close relations between them. Cyberspace is not a closed, hermetic entity within information space. However, we can also begin to formulate questions: does information space contain the whole of cyberspace? Thus, ought we to speak of inclusion or of intersection?

The principle of the different levels (layers, strata, dimensions), of which there tend to be three, in information space, cyberspace or the electromagnetic domain, is then applied to various objects – e.g. resilience analysis. We can also supplement the three dimensions. Daniel A. Eisenberg[52], in his approach to resilience, adopts a framework with four different levels: physical, informational, cognitive and social. Note that this more complex rendering of the model reflects the awareness of the imperfection of the three-layer model, which is probably incomplete, and also the difficulty theorists have in reaching agreement both as to the limitations and the overlaps between those layers, and their ability to model, represent and map these artificial "spaces".

4.2.2. *Definitions and models for information warfare*

In regard to the models presented in the last section (section 4.2.1), information operations and/or information warfare are situated in information space in general, and borrow cyberspace (where they are not focused on the psycho–cognitive layer – content, ideas, domain of influence – but in fact require action to be taken on all the other levels). Information warfare is waged on all levels: a cyber attack (layer 2) will produce psychological effects; an attack on the physical infrastructure may also cause these same effects; countering psychological maneuvers and propaganda or influencing efforts will also involve acting on the application layer (e.g. carrying out cyber attacks against propaganda sites; infiltrating computers/servers/ systems in order to extract information; etc.).

52 Daniel A. Eisenberg *et al.*, "Resilience metrics: lessons from military doctrines", *The Solutions Journal*, vol. 5, no. 5, pp. 76–87, October 2014, http://www.thesolutionsjournal.com/node/237200.

Thus, there is a permanent relation between cyber operations and information warfare/information operations, but also between operations in the EM spectrum and information warfare. Thus, FM 3-38 (USA)[53] posits the existence of crosslinks between the EM spectrum, cyberspace and the information environment. The latter encapsulate cyberspace and the electromagnetic spectrum: "cyberspace and the EMS are part of the information environment"[54]. The report goes on to specify that CEMA (Cyber Electro Magnetic Activities) apply to each of the three dimensions of the information environment, either directly or indirectly. Thus, "while cyberspace and the EMS do not exist within the cognitive dimension", actions conducted in the other dimensions can have an effect on the cognitive layer[55].

Information warfare operations will thus be conducted in the following 9 arenas of action:

	Information environment		
	Information (part other than cyber and EM)	Cyberspace	EM domain
Physical	Supports, vectors of production and distribution	Information infrastructures, networks, systems, hardware	Information infrastructures, telecoms, hardware
Application, software/information/data	Information/data	Information/data/ software applications	Signals
Cognitive/social	Content, meaning, individuals	Content, meaning, individuals	

Table 4.4. *Information warfare operations in the information environment*

53 http://fas.org/irp/doddir/army/fm3-38.pdf.
54 Page I-6.
55 Given that the electromagnetic spectrum is considered to be one of the components of information space, it too inherits the same general three-dimensional structure.

The diagrams below illustrate the interactions between the layers, enabling us to envisage multiple scenarios of operations.

Cyberattacks across all three layers

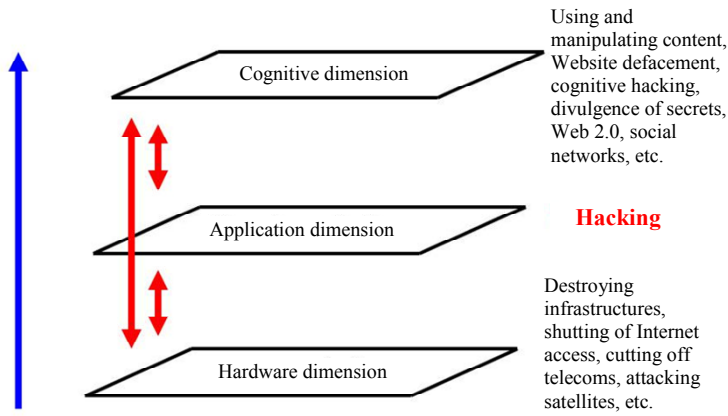


Figure 4.5. *Interactions between the various layers of cyberspace*

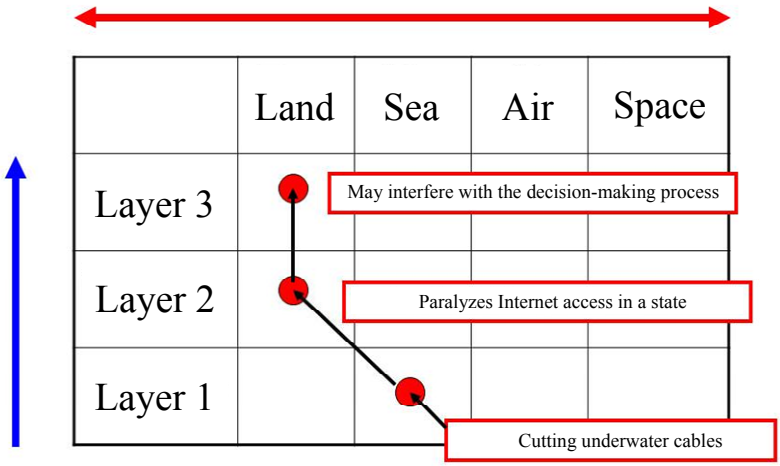


Figure 4.6. *Cyber attack and cyberspace matrix/grid*

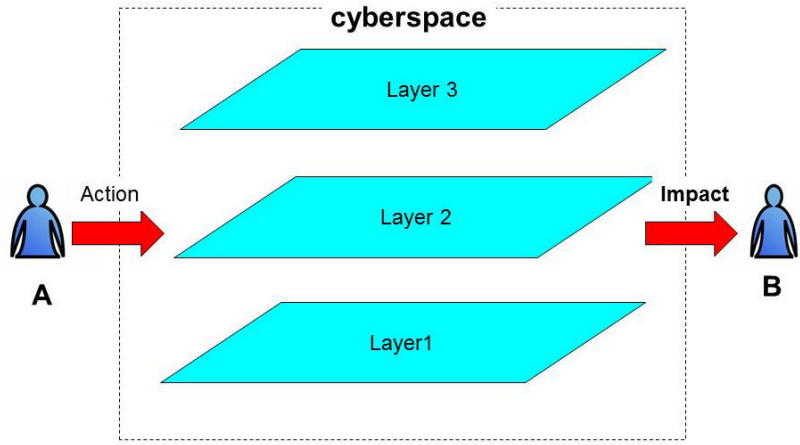


Figure 4.7. *Most important of all: the effect that A can have on B*

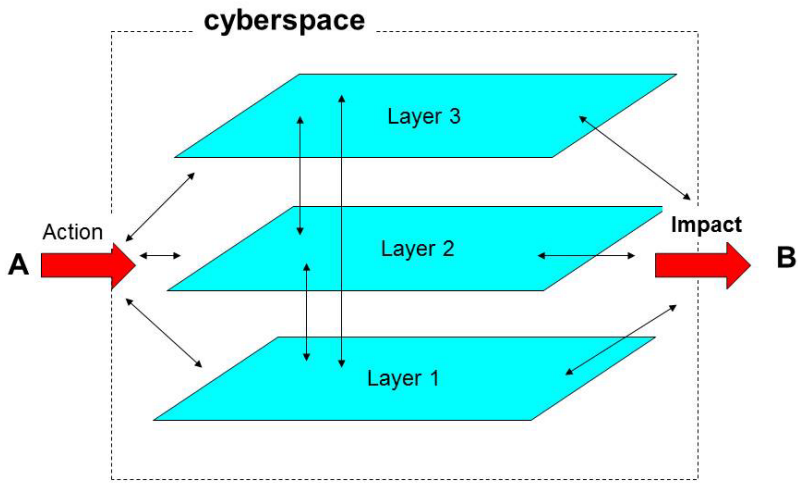


Figure 4.8. *Actions taken on one layer may have impacts on the other layers, or be combined with actions on the other layers of cyberspace*

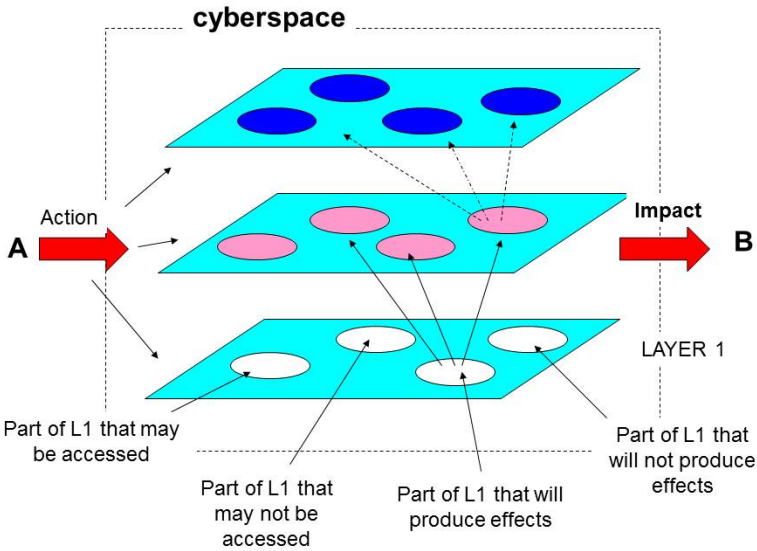


Figure 4.9. *On each layer, the actions may be limited by a variety of factors: certain parts of these layers may be inaccessible, or may not be the best bath to take to produce effects*

Is it necessary to redefine information warfare? This is the question that many researchers have been asking in recent years. Timothy L. Thomas[56] wonders about the evolution of the paradigm, its definition and its place in the area of defense concepts. A study by the RAND Corporation, published in 2013, proposes a redefinition of the boundaries of information warfare to take account of the evolutions of the connected world[57]. Patricia H. Williams[58] deems it relevant to examine this definition, which has been constantly evolving over the

56 Timothy L. Thomas, "Is the IW paradigm outdated? A discussion of U.S. IW theory", *Journal of Information Warfare*, vol. 2, no. 3, pp. 109–116, 2003.

57 Isaac R. Porche III *et al.*, "Redefining Information Warfare Boundaries for an army in a wireless world", Rand Corporation, United States, 2013, http://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf.

58 Patricia A H Williams, "Information Warfare: Time for a redefinition", Edith Cowan University, Research Online, Australia, 2010, http://www.researchgate.net/profile/Patricia_Williams10/publication/49279651_Information_Warfare_Time_for_a redefinition/links/09e415121830739c6b000000.pdf

course of the past 20 years – especially given that the boundaries of cybersecurity do not overlap with those of information warfare: "cyber security is a general term that covers all aspects of attack protection, and is not specifically an information warfare topic"[59]. Information warfare, she points out, first changed in terms of its composition, in view of the technological evolution. Then, information warfare techniques emerged from the military domain (information warfare was a separate discipline, with primarily–military implications, and even within the forces, around the turn of the millennium, it underwent a significant change, with the progress of information technologies and the military's increased dependency on their computer systems), and began to be applied in other environments (notably economic). Information warfare must, in any case, be understood in the broader context of security issues. According to Patricia H. Williams, the fundamental principles, the components of information warfare, have not changed over the last two decades (the fundamentals remain the same: defensive and offensive operations, espionage, judicial and ethical issues, propaganda and intelligence). What has changed is the context in which information warfare takes place (and the new issues questions at the center of the debate, such as cybersecurity, protection of critical infrastructures, cyberterrorism, etc.), with the marking fact being the duplication or transfer of military techniques, methods and tools to the civilian and social sphere (a phenomenon which had already been noted several years earlier by other authors)[60]. One of the consequences, Williams continues, is likely to be overexposure of society to terrorism, for example – particularly to cyberterrorism, where two phenomena are linked: the number of actors who have access to offensive capabilities and society's dependence on information systems).

---

59 Patricia A H Williams, "Information Warfare: Time for a redefinition", Edith Cowan University, Research Online, Australia, 2010, http://www.researchgate.net/profile/Patricia_Williams10/publication/49279651_Information_Warfare_Time_for_a_redefinition/links/09e415121830739c6b000000.pdf

60 B. Cronin, H. Crawford, "Information Warfare: its application in military and civilian contexts", *The Information Society*, no. 15, pp. 257–263, 1999.

Source	Definition	Dates
Winn Schwartau[61]	Defines three classes of information warfare: 1. Personal Information Warfare 2. Corporate Information Warfare 3. Global Information Warfare "Information Warfare is an electronic conflict in which information is a strategic asset worthy of conquest or destruction. Computers and other communications and information systems become attractive first–strike targets".	1994
US Joint Chiefs of Staff[62]	"IW focuses on affecting an adversary's information environment while defending our own".	1995
Martin Libicki[63]	"Information warfare, as a separate technique of waging war, does not exist. There are, instead, several distinct forms of information warfare, each laying claim to the larger concept. Seven forms of information warfare–conflicts that involve the protection, manipulation, degradation, and denial of information–can be distinguished: (i) command-and-control warfare (which strikes against the enemy's head and neck), (ii) intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace), (iii) electronic warfare (radio–electronic or cryptographic techniques), (iv) psychological warfare (in which information is used to change the minds of friends, neutrals, and foes), (v) "hacker" warfare (in which computer systems are attacked), (vi) economic information warfare (blocking information or channeling it to pursue economic dominance), and (vii) cyber warfare	1995

61 Winn Schwartau, *Information Warfare, Chaos on the Electronic Superhighway*, Thunder's Mouth Press, 1994.
62 Cited in Isaac R. Porche III *et al.*, "Redefining Information Warfare Boundaries for an army in a wireless world", Rand Corporation, United States, 2013.
63 Martin Libicki, What is Information Warfare?; Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS), Washington, 1995, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662.

	(a grab bag of futuristic scenarios). All these forms are weakly related".	
Richard Szafransky[64]	"Information warfare is hostile activity directed against any part of the knowledge and belief systems of an adversary".	1995
The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) Number 3210.01, dated 02 January 1996. Paragraph 5, Definitions	"Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information based processes, information systems, and computer-based networks". Information Systems are "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information".	1996
CJCSI 3210.01	"Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer based networks while defending one's own information, information-based processes, information systems and computer-based networks".	1996
J.I. Alger[65]	"Actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary".	1996
Wang Boacun and Li Fei[66]	"Information warfare in the narrow sense refers to the U.S. military's so-called battlefield information warfare, the crux of which is command and control warfare. It is defined as the comprehensive use, with	1997

64 Richard Szafransky, "A theory of information warfare, preparing for 2020", *Airpower Journal*, Spring 1995.

65 J.I. Alger, "Introduction", In *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*, W. Schwartau (ed.), 2nd edition, New York: Thunder's Mouth Press, 1996.

66 Wang Boacun, Li Fei. "Information Warfare", in Michael Pillsbury, (ed.), *Chinese Views of Future Warfare*, Washington, DC, National Defense University Press, 1997, http://fas.org/irp/world/china/docs/iw_wang.htm.

	intelligence support, of military deception, operational secrecy, psychological warfare, electronic warfare, and substantive destruction to assault the enemy's whole reformation system including personnel; and to disrupt the enemy's information flow, in order to impact, weaken, and destroy the enemy's command and control capability, while keeping one's own command and control capability from being affected by similar enemy actions".	
Wang Boacun and Li Fei[67]	"Information warfare in the broad sense refers to warfare dominated by information in which digitized units use information [smart] equipment. While warfare has always been tied to information, it is only when warfare is dominated by information that it becomes authentic information warfare".	1997
A. Borden[68]	Information warfare encompasses C2 operations, psychological operations, offensive and defensive operations in the informational domain.	1999
Megan Burns[69]	Information warfare is "a class of techniques, including collection, transport, protection, denial, disturbance, and degradation of information, by which one maintains an advantage over one's adversaries"[70].	1999

67 Wang Boacun, Li Fei. 'Information Warfare", in Michael Pillsbury (ed.), *Chinese Views of Future Warfare*, Washington, DC, National Defense University Press, 1997, http://fas.org/irp/world/china/docs/iw_wang.htm.

68 A. Borden, "What is Information Warfare?", *Air & Space Power Journal*, 1999.

69 Megan Burns, Information Warfare: what and how?, http://www.cs.cmu.edu/~burnsm/InfoWarfare.html, 1999.

70 Megan Burns identifies the following components of information warfare:

- Weapons of information warfare: information collection, information transport, information protection, information manipulation, information disturbance, degradation and denial;
- Defending against information warfare: information collection, information transport, information protection, information manipulation, information disturbance, degradation and denial.

Xie Guang[71]	"IW in military sense means overall use of various types (of) information technologies, equipment and systems, particularly his command systems, to shake determination of enemy's policy makers and at the same time, the use of all the means possible to ensure that that one's own systems are not damaged or disturbed".	1999
Hutchinson & Warren[72]	A situation in which information "has to be manipulated to the advantage of those trying to influence it".	2001
Department of Defense (USA)[73]	"Information operations conducted during time of crisis of conflict to achieve or promote specific objectives over a specific adversary or adversaries […] information operations – Actions taken to affect adversary information and information systems while defending one's own information and information systems".	2001
Brian Nichiporuk[74]	"The process of protecting one's own sources of battlefield information and, at the same time, seeking to deny, degrade, corrupt, or destroy the enemy's sources of battlefield information […] This is taken to include six preexisting subareas […] operational security, electronic warfare (EW), psychological operations (PSYOPs), deception, physical attack on information processes, and information attack on information processes".	2002

71 Cited in Vinod Adan, "Chinese concepts and capabilities of information warfare", *Strategic Affairs*, vol. 30, Issue 4, October 2006, http://www.idsa.in/strategicanalysis/ChineseConceptsandCapabilitiesofInformationWarfare_vanand_1006.

72 W. Hutchinson, M. Warren, 'Principles of Information Warfare", *Journal of Information Warfare*, no. 1, pp. 1–6, vol. 1, 2001.

73 Department of Defense, Dictionary of Military and Associated Terms, Joint Pub 1-02. April 12, 2001, http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf.

74 Brian Nichiporuk, "U.S. military opportunities: information-warfare concepts of operations", in Zalmay Khalilzas, Jeremy Shapiro, Strategic Appraisal: United *States Air and Space Power in the 21st Century, RAND Corporation*, 2002, http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1314/MR1314.ch6.pdf.

Daniel Ventre	The aggressive/defensive use of information space components (which are information and information systems) to reach/protect the sovereignty of a nation through actions conducted in times of peace, crisis or conflict[75].	2008
Patricia A H Williams	"Information warfare is also referred to as cyberwar, network centric warfare, information operations and command and control warfare. In today's definition, information warfare incorporates all of these"[76].	2010
Patricia A H Williams	"Using information to make decisions and for the adversary, trying to influence, deny, or disrupt information used in decision making processes"[77].	2010
Patricia A H Williams	"The current definitions include areas such as specific information infrastructure attack, cyber terrorism, cyber crime, attacks on commercial and military web sites, website defacement, cyber war, netwar, denial of service attacks and so on"[78].	2010
Rand Corporation[79]	"Information warfare is conflict or struggle between two or more groups in the information environment".	2013
Dan Kuehl[80]	"Military offensive and defensive actions to control/exploit the environment".	2013

75 Daniel Ventre, "Guerre de l'information : la prolifération des capacités?" *Défense et Sécurité Internationale Review* (*DSI*), no. 38, pp. 30–35, June 2008.
76 Patricia A H Williams, "Information Warfare: Time for a redefinition", Edith Cowan University, Research Online, Australia, p. 10, 2010, http://www.researchgate.net/profile/Patricia_Williams10/publication/49279651_Information_Warfare_Time_for_a_redefinition/links/09e415121830739c6b000000.pdf.
77 *Idem*.
78 *Idem*.
79 Isaac R. Porche III *et al.*, "Redefining Information Warfare Boundaries for an army in a wireless world", Rand Corporation, United States, 2013, http://www.rand.org/content/dam/rand/pubs/monographs/MG1100/MG1113/RAND_MG1113.pdf.
80 Cited in Isaac R. Porche III *et al.*, "Redefining Information Warfare Boundaries for an army in a wireless world", Rand Corporation, United States, p. 178, 2013.

Jolanta Darczewska[81]	"Russian authors understand 'information warfare' as influencing the consciousness of the masses as part of the rivalry between the different civilizational systems adopted by different countries in the information space by use of special means to control information resources as 'information weapons'"[82].	2014
Nadiya Serskykh[83]	Information warfare – the use and management of information in order to obtain a competitive advantage over the enemy. Information warfare may include: – gathering tactical information; – security of their information resources; – spreading of propaganda or disinformation to demoralize the army and the public enemy; – undermining the quality of information and warning of enemy capabilities information gathering opponent. The concept of "information warfare" necessarily includes the concept of "information weapons". This definition is not the same as that of "military" information warfare, but applies to the economic sector.	2014
Mariarosaria Taddeo[84]	"Information warfare is the use of ICTs within an offensive or defensive military strategy endorsed by a	2014

81 Jolanta Darczewska, "The anatomy of Russian information warfare. The Crimean operation, a case study", *Point of View*, Poland, no. 42, p. 37, May 2014,: http://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf.
82 Jolanta Darczewska also stresses that the Russian approach combines military and non-military, technological space (cyberspace) and social (information space). She also refers explicitly to the Cold War, to the psychological war between the Eastern and Western Blocs. Cyberspace is merely a subset, and cybersecurity is one issue within a broader set of objectives. Matters pertaining to cyber seem to be more confidential.
83 Nadiya Serskykh, Information Wars in the Internet Marketing Context, p. 4, 2014, http://nbuv.gov.ua/j-pdf/znptdau_2014_2_7.pdf.

	[political authority] and aimed at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging across the physical and non–physical domains and whose level of violence may vary upon circumstances".	
Rianne van Vuuren[85]	"Information warfare is defined as actions focused on destabilising or manipulating the core information networks of a state or entities in society with the aim to influence the ability and will to project power as well as efforts to counter similar attacks by an opposing entity and/or state".	2015

Table 4.5. *Selection of definitions of "information warfare"*

Michael Raska (RSIS, Singapore) discusses the three forms of information conflicts (making up information warfare), which are: war 1) by means of, 2) for and 3) against information, basing his remarks on the observation of the means of conflict between North and South Korea: "North and South Korea engage in three information conflicts simultaneously – a war for information to obtain information and intelligence about each other's means, capabilities and strategies; a war against information aimed at protecting their information systems, while disrupting or destroying the other side's information infrastructure; and a war through information reflected in the misinformation and deception operations to shape their broader internal and external strategic narratives"[86]. To express the evolution of information warfare, of its outlines and its modes, Raska introduces

84 Mariarosaria Taddeo, "Information warfare: the ontological and regulatory gap", *APA Newsletter on Philosophy and Computers*, p. 16, 2014, https://mariarosariataddeo.files.wordpress.com/2014/02/apa-cyberwarfare-preprint.pdf.

85 Rianne van Vuuren, "A Futures Model to Address Information Warfare as an Upcoming Wicked Problem, Futures Studies Tackling Wicked Problems: Where Futures Research, Education and Action meet", p. 23, 11–12 June 2015, https://futuresconference2015.files.wordpress.com/2015/06/rianne-van-vuuren.pdf.

86 Michael Raska, Integrating information warfare into U.S.-ROK defence strategy, 2013: http://www.michaelraska.de/download/M_Raska_Korea_Herald_IW.pdf.

two formulae: information warfare 3.0 and Weapons of Mass Effectiveness (WMEs)[87], which are a combination of elements of cyber warfare and information warfare.

Components	Targets	Actors
– mass–media information denial, disruption, destruction and manipulation campaigns, – confrontations in cyberspace, – attacks on computerized systems, – cyber attacks on physical infrastructure systems, – cyber espionage, – electronic warfare – perception management	– traditional governmental bureaucracies, – intelligence agencies – military organizations	– individuals, – states and non-state networks

Table 4.6. *Information warfare 3.0 and WMEs, from Michael Raska, 2013*[88]

Megan Burns[89] identifies five components of information warfare (see Table 4.7), organized around the two axes of offensive and defensive. In her defensive approach, Burns includes a number of offensive measures:

87 Michael Raska, Information warfare 3.0: Weapons of mass effectiveness, The Nation, Singapore, 3 July 2013, http://www.nationmultimedia.com/opinion/Information-warfare-3-0-Weapons-of-mass-effectiven-30209538.html.

88 Michael Raska, Information warfare 3.0: Weapons of mass effectiveness, The Nation, Singapore, 3 July 2013, http://www.nationmultimedia.com/opinion/Information-warfare-3-0-Weapons-of-mass-effectiven-30209538.html.

89 Megan Burns, Information Warfare: what and how?, 1999: http://www.cs.cmu.edu/~burnsm/InfoWarfare.html.

	Information collection	Information transport	Information protection	Information manipulation	Information disturbance, degradation and denial
Weapons of Information Warfare	To infiltrate situations and gather accurate information with minimal loss of fidelity	Ability to transport information into the hands of those who need it	To minimize the amount of information to which your opponent has access.	The alteration of information with intent to distort the opponent's picture of reality	Preventing the enemy from getting complete, correct information
Defending against information warfare	To prevent our enemies from assembling information about us and about the conflict situation.	The most effective countermeasure for preventing transport is the destruction of the enemy's infrastructure	To counteract enemy attempts to protect their own information supply, we must be able to get around their protection mechanisms	Preventing the enemy from intercepting information in the first place. Preventing the altered data from being re-introduced into the flow of real information.	Requires the use of many of the countermeasures already mentioned

Table 4.7. *Components of information warfare. Reconstructed from Megan Burns, 1999*[90]

Numerous attempts to model the processes of information operations or information warfare are inspired by the OODA loop, from which they adopt the logic of successive inter-chained phases –

90 Megan Burns, Information Warfare: what and how?, 1999: http://www.cs.cmu.edu/~burnsm/InfoWarfare.html.

see, for example, the models put forward in 2011 by Brett van Niekerk and Manoj S. Maharaj[91].

In 2009, in the first edition of this book, the author proposed the following model, identifying a cycle of successive phases, all causing effects on one another.

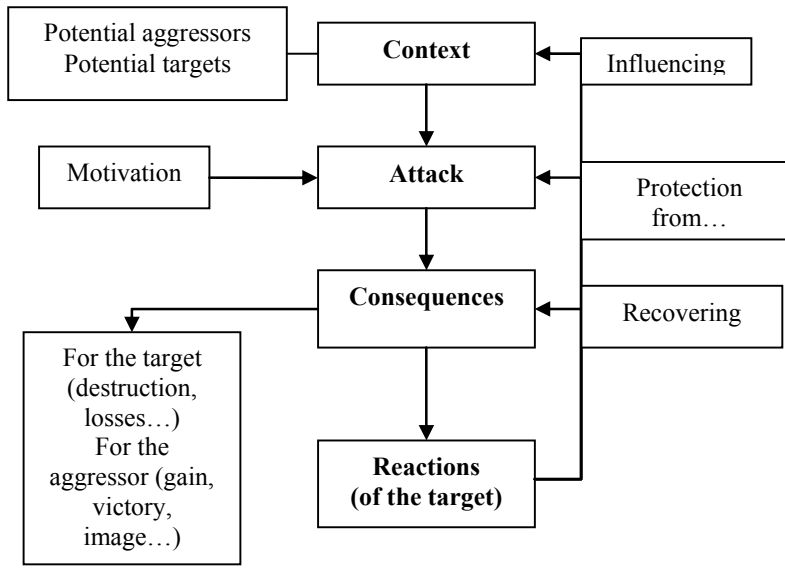


Figure 4.10. *Context – attack – consequences – reactions cycle*

In the view of Rianne van Vuuren[92], information warfare is based on three components – netwar, cyber warfare and psychological operations.

91 Brett van Niekerk, Manoj S. Maharaj, "The Information Warfare LifeCycle Model", *Journal of Information Management*, South Africa, vol. 13, no. 1, 2011, http://www.sajim.co.za/index.php/SAJIM/rt/suppFiles/476/0.

92 Rianne van Vuuren, "A Futures Model to Address Information Warfare as an Upcoming Wicked Problem, Futures Studies Tackling Wicked Problems: Where Futures Research, Education and Action meet", 11-12 June 2015, https://futuresconference2015.files.wordpress.com/2015/06/rianne-van-vuuren.pdf.

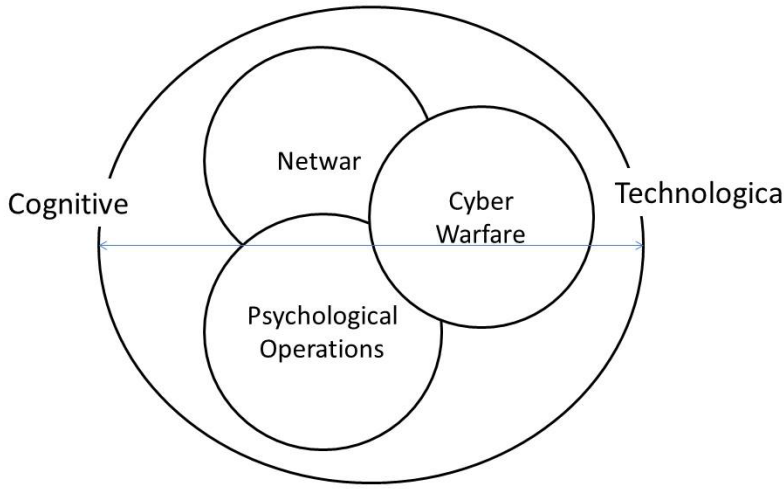


Figure 4.11. *Information warfare, as described by Rianne van Vuuren, 2015*[93]

	Russia	China	USA
Cyber warfare	"Combat actions in cyberspace are cyber attacks carried out by states, groups of states, or organised political groups, against cyber infrastructure, which are part of a military campaign"[94].	Both for Russia and for China, this term refers essentially to Western practices.	"Cyber warfare is cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with a government campaign"[95].

93 Rianne van Vuuren, "A Futures Model to Address Information Warfare as an Upcoming Wicked Problem, Futures Studies Tackling Wicked Problems: Where Futures Research, Education and Action meet", 11-12 June 2015, https://futuresconference2015.files.wordpress.com/2015/06/rianne-van-vuuren.pdf.

94 Russia–U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, East West Institute, April 2011, http://www.ewi.info/cybersecurity-terminology-foundations.

95 *Idem*.

Information space	"The sphere of activity connected with the formation, creation, conversion, transfer, use, and storage of information and which has an effect on individual and social consciousness, the information infrastructure, and information itself"[96].	"The main function of the information space for people to acquire and process data... a new place to communicate with people and activities, it is the integration of all the world's communications networks, databases and information, forming a 'landscape' huge, interconnected, with different ethnic and racial characteristics of the interaction, which is a three–dimensional space"[97].	
Cyberspace			A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer

96 Russia–U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, East West Institute, April 2011, http://www.ewi.info/cybersecurity-terminology-foundations.
97 H.B. Wasuo, *Information Space*, Shanghai, Translation Publishing House, 2000.

			systems, and embedded processors and controllers[98].
Information weapon	"Propaganda carried out using the mass media is the most traditional and most powerful general–purpose information weapon... Information weapons are being actively developed at the present time based on programming code... Information weapons also include means that implement technologies of zombification and psycholinguistic programming"[99].		Term not frequently used in the English–speaking world, according to the authors. The expression is set apart from "cyber weapon", which is felt to be more Western. We do not agree with this observation. The literature on information warfare builds a large number of its arguments around the fact that information is simultaneously a target and a weapon[100].
Information warfare	"Information war is the deliberate teaching of your enemy how to remove his own shell"[101].		"Information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy, an adversary's information,

98 Joint Chiefs of Staff, Department of Defense, Dictionary of Military and Associated Terms, Joint-Publication 1-02, 8 November 2010 (as amended through 15 June 2015), 469 pages, United States, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

99 Fedorov, Tsigichko, Information Challenges to National and International Security, Moscow, PIR Centre, 2001.

100 Kelly Fisher, "Emerging ethical issues: universities and information warfare", *Journal of Academic and Business Ethics*, p. 10, July 2013: http://cryptome.org/2013/07/cyber-war-racket-0030.pdf.

101 S. Rastorguyev, Information War, Problems and Models, Moscow, 2006.

			information–based processes, information systems, and computer–based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries[102].

Table 4.8. *Comparison of the definitions of a number of key concepts, from Keir Giles, William Hagestad (2013)[103]*

Information warfare is founded on the exploitation of all three dimensions of the information space (just as cyberspace operations will also be based on these three dimensions).

Target	Actions
Physical assets	Damage or destroy target's information and communication systems using conventional warfare techniques
Soft assets	Infiltrate, degrade, subvert information systems; use external actors and corrupted insiders to crack firewalls and degrade target's information systems capability, using malicious software
Psychic assets	Silent penetration of target's information and communications systems to manage perceptions, shape opinions, foster deception, and engage in epistemological warfare

Table 4.9. *The three layers of the information environment and the actions of information warfare on each of the layers. From Blaise Cronin and Holly Crawford, 1999[104]*

102 J. Arquilla, J., D. Ronfeldt, Cyberwar is Coming! Comparative Strategy, 12 (2), pp. 141–160, 1993.

103 Keir Giles, William Hagested, "Divided by a common language: cyber definitions in Chinese, Russian and English", *5th International Conference on Cyber Conflict*, NATO CCD COE, Tallin, 2013, https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf.

104 Blaise Cronin and Holly Crawford, "Information Warfare: Its Application in Military and Civilian Contexts", *The Information Society*, 15, pp. 257–263, 1999: http://www.indiana.edu/~tisj/readers/full-text/15-4%20cronin.pdf.

4.3. Information warfare or data warfare?

In recent years, many publications have been devoted to the necessity of redefining information warfare. In light of the technical evolutions, the changes in practices over the past 20 years, the evolution of conflicts themselves (in terms of their form, their nature), the boundaries of information warfare may have shifted somewhat – particularly because of the predominant role seemingly played by the cybernetic dimension of the conflict. Yet the predominance of data is probably an adjustment variable to be taken into consideration in this task of reformulation.

In 1995, Martin Libicki stated that the popularity of the concept of information warfare, at the time, could be attributed to the increasingly prevalent place occupied by information and information technologies in the field of national security[105].

Should we, today, not reformulate this observation, replacing "information" with "data", and "information technologies" with "data technologies", given that such hope is placed in these technologies, and their role in security matters has become so important? After all, the aim is to protect citizens' private lives, to ensure security and national defense from various categories of threats (crime and terrorism, but also climatic, environment, sanitary (etc.) challenges), data play a central role. Edward Snowden's revelations shed light on the extent of data–harvesting practices, illustrating the major role that data play in security– and defense policies. The consequences of large–scale losses and theft of data (personal, industrial, military, criminal, etc.) are becoming apparent, and we are beginning to realize how important data are in people's financial and social lives, even in their very destiny. The technological evolutions that are underway are transforming every citizen and every object into a data sensor or a data

105 "In recent years, a concept known as 'information warfare' has become popular within certain circles of the U.S. defense establishment. The concept is rooted in the indisputable fact that information and information technologies are increasingly important to national security in general and to warfare specifically". From Martin Libicki, What is Information Warfare?; Directorate of Advanced Concepts, Technologies, and Information Strategies (ACTIS), Washington, p. 110, 1995, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662

source, a user and consumer of data: drones, robotics, neural interfaces, Internet of Things, smart cities, etc. – all of this constructs an environment which does not directly produce information, but rather a halo of data.

In today's world, data are at the heart of the economy, of national security matters, of the evolution of cyberspace and of society itself. The concept is ubiquitous, and the notion of "data" has infinite offshoots: open data, big data, data mining, data scientist, data science, data animator, data sources, data representations, data centers, data security, data flaw, navigation data, raw data, metadata, database, false data, targeting data, corrupting the data, data breach, data analytic, personal data, data visualization, data protection act, and so on. There is an abundance of published works on the subject of data: on how to make data "talk" by statistical treatments; on data mining; on computer graphics (Charles Wheelan, 2014[106]; Foster Provost, 2013[107]; John W. Foreman, 2013[108]); on the power of data which, when combined with modern processing tools, can reveal information and knowledge; on predictive analysis; on decision supports; on controlling the actors involved; on markets (Eric Siegel, 2013[109]; Bart Baesens, 2014[110]; Bernard Marr, 2015[111]; Steve Lohr, 2015[112]); on the interest held by data, their value (Jared Dean, 2014[113]; Lillian Ablon, Martin C. Libicki, 2014[114]); on data as a marker of individual rights

106 Charles Wheelan, *Naked Statistics: Stripping the Dread from the Data*, W.W. Norton 2014.

107 Foster Provost, *Data Science for Business: What you need to know about data mining and data-analytic thinking*, O'Reilly Media, 2013.

108 John W. Foreman, *Data Smart: Using Data Science to Transform Information into Insight*, Wiley, 2013.

109 Reic Siegel, *Predictive Analytics: the Power to Predict Who will Click, Lie or Die*, Wiley, 2013.

110 Bart Baesens, *Analytics in a Big Data World: the Essential Guide to Data Science and its Applications*, Wiley, 2014.

111 Bernard Marr, *Big Data: Using Smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance*, Wiley, 2015.

112 Steve Lohr, *Data-ism: the revolution transforming decision making, consumer behavior, and almost everything else*, Harper Business, 2015.

113 Jared Dean, *Big Data, Data Mining, and Machine Learning*, Wiley, 2014.

114 Lillian Ablon, Martin C. Libicki, "Markets for cybercrime tools and stolen data: hackers' bazaar", *Rand Corporation*, Santa Monica, California, 2014.

(privacy) (Bruce Schneier, 2015[115]); on data as the object upon which the modern economy hinges (we frequently heart the expression "data-driven") (Carl Anderson, 2015[116]; Paul Bambrick–Santoyo, 2010[117]; Jenny Dearborn, 2015[118]; Jay Jacobs, Bob Rudis, 2014[119]). The new-found popularity of computer graphics – a discipline which lies somewhere between science, technology and art, which helps shed new light on data and on the world – feeds our voracious appetite for data (Nathan Yau, 2011[120], 2013[121]; David McCandless, 2012[122], 2014[123]; Zach Gemignani *et al.*, 2014[124]). However, an interest in data, recognition of their specific status and value, is not a new phenomenon. Since the 1970s–1980s, data have been fueling legal debates, with numerous states constructing legal corpora that help to protect their data (particularly personal/identifying data) and the actors attached to them. In the existing body of literature we find articles, reports, studies and books on the protection of data, of privacy, of identity, and on the right to regulate international data streams. Snowden's revelations about states' surveillance practices were based not only on issues about the nature of the relationships between states, but also on the rights of individuals; of citizens; their fundamental freedoms; the rights of the security, defense and intelligence agencies,

115 Bruce Schneier, *Data and Goliath: the hidden battles to collect your data, and control your world*, W. W. Norton 2015.

116 Carl Anderson, *Creating a data-driven organization*, O'Reilly Media, 2015.

117 Paul Bambrick-Santoyo, *Driven by Data: a practical guide to improve instruction*, Jossey-Bass, 2010.

118 Jenny Dearborn, *Data Driven: how performance analytics delivers extraordinary sales results*, Wiley, 2015.

119 Jay Jacobs, Bob Rudis, *Data-driven security: analysis, visualization and dashboards*, Wiley, 2014.

120 Nathan Yau, *Vizualise this: the FlowingData guide to design, visualization, and statistics*, Wiley, 2011.

121 Nathan Yau, *Data Points: visualization that means something*, Wiley, 2013.

122 David McCandless, *Visual Miscellaneum: The Bestselling Classic, Revised and Updated: A Colorful Guide to the World's Most Consequential Trivia*, Harper Design, 2012.

123 David McCandless, *Knowledge Is Beautiful: Impossible Ideas, Invisible Patterns, Hidden Connections–Visualized*, Harper Design, 2014.

124 Zach Gemignani *et al.*, *Data fluency: empowering your organization with effective data communication*, Wiley, 2014.

faced with the security versus freedom dilemma. In these debates, the concept of "data" was crucially important: which data can legally be brought to states' attention; which data must remain in the private, inviolable sphere of the individuals; which information and which intelligence can states truly hope to extract by their practices of "mass" data collection; do mass collect and mass treatment guarantee effective security?

4.3.1. *Defining data*

Data are in the process of ousting information, to the extent where we can qualify ours as no longer being the "information society", but rather the "data society".

Data represent the raw material, the resource, which feeds and flows through our systems, the global network of communications between individuals, between machines and systems. Companies produce data, as do individual citizens, institutions, and the technical systems themselves; data have acquired a market value, a strategic value, so people steal them and resell them; they are a target. For the past two decades, databases have been falling victim to mass theft. Data are the central element in the debates, which have become controversial in recent years, about the practices of intelligence agencies; about the practices of surveillance and collection of citizens' data by states and enterprises; the merchant sector; the tension between privacy, freedom and national security, the practices of mass surveillance, and espionage.

The progress in science and technology has given rise to new data-processing tools, and opened up the way to new practices and new treatments. The whole of our environment, in the industrialized world, is built around data, with their multiplication or the proliferation of sensors, of networks, of processing tools: open data, big data, the Internet of Things, smart cities, robots, neural interfaces, etc. create data in previously unheard of quantities.

When data describe the world and enable us to see it differently, and data processing tools allow us to predict, warn, anticipate and reveal

secrets which have hitherto been beyond the reach of science, they become the object of desire. It is helpful to dominate and control data. With this in mind, we need to be able to collect data and control the flow of them, the technological infrastructure, the software/application layer of the treatments, but also to secure and defend those data.

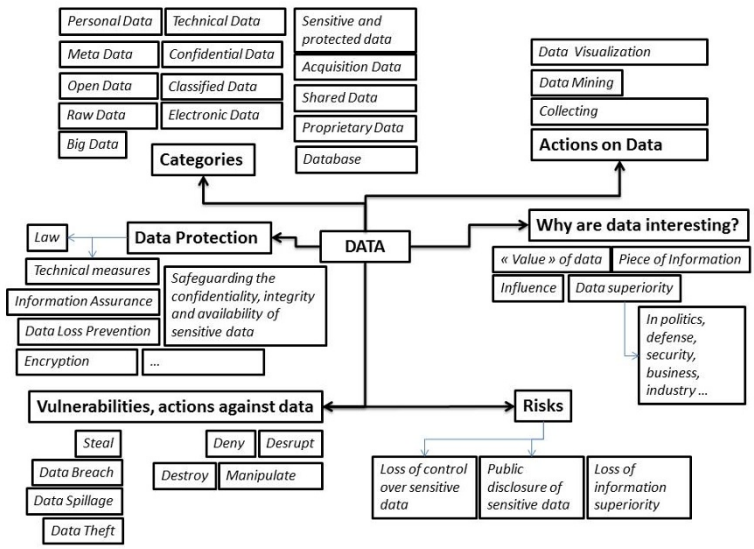


Figure 4.12. *Data categories, actions, roles, protection*

Definition of data (and its relationship to information)	Source	Date
"Data is raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized […] Data are simply facts or figures – *bits* of information, but not information itself". "When data are processed, interpreted, organized, structured or presented so as to make them meaningful or useful, they are called information. Information provides context for data".	www.diffen.com[125]	No date

125 http://www.diffen.com/difference/Data_vs_Information.

"Information is the end product of data processing".	Margaret Rouse[126]	No date
"Information is data that has been processed into a form that is meaningful to the recipient".	Davis Olson[127]	1985
Data and information can be treated as being roughly the same thing: "Broadly speaking the DPA covers four types of information (referred to as 'data' in the Act)"[128].	Data Protection Act (UK)	1998
"In computational systems data are the coded invariances. In human discourse data are that which is stated, for instance, by informants in an empirical study".	Cited by Chaim Zins[129]	2007
"Data is a symbol set that is quantified and/or qualified".	Cited by Chaim Zins	2007
"Data are sensory stimuli that we perceive through our senses".	Cited by Chaim Zins	2007
"The word "data" is commonly used to refer to records or recordings encoded for use in computer, but is more widely used to refer to statistical observations and other recordings or collections of evidence".	Cited by Chaim Zins	2007
"Data are the basic individual items of numeric or other information, garnered through observation; but in themselves, without context, they are devoid of information".	Cited by Chaim Zins	2007
"Data are symbols organized according to established algorithms".	Cited by Chaim Zins	2007
"Raw data (sometimes called source data or atomic data) is data that has not been processed for use".	Cited by Chaim Zins	2007

126 Margaret Rouse, Raw data (sometimes called source data or atomic data) is data that has not been processed for meaningful use, no date: http://searchdatamanagement.techtarget.com/definition/raw-data.

127 G.B. Davis, M.H. Olson, *Management information systems*, New York, McGraw Hill, 1985.

128 Data Protection Act 1998, United Kingdom, https://ico.org.uk/media/for-organisations/documents/1549/determining_what_is_personal_data_quick_reference_guide.pdf

129 Chaim Zins, "Conceptual Approaches for Defining Data, Information, and Knowledge", *Journal of the American Society for Information Science and Technology*, vol. 4, pp. 479–493, 2007: http://web.simmons.edu/~weigle/ISEL%20ISIC%20ATTITUDES/zins_definitions_dik.pdf.

"Data can be defined as a class of information objects, made up of units of binary code that are intended to be stored, processed, and transmitted by digital computers".	Cited by Chaim Zins	2007
"Data are facts and statistics that can be quantified, measured, counted, and stored. Information is data that has been categorized, counted, and thus given meaning, relevance, or purpose".	Cited by Chaim Zins	2007
"Data are the raw observations about the world collected by scientists and others, with a minimum of contextual interpretation. Information is the aggregation of data to make coherent observations about the world".	Cited by Chaim Zins	2007
"Data: raw, frequently unstructured items apart from context or interpretation. Data are the first link between an IS and the DIKW[130] hierarchy. People use an IS to interact with the data". "Information: data that have been transformed to have meaning for human beings by being organized with specific relationships between the data".	Harry D. Tunnell[131]	2014
"Data. Interpreted signals that can reduce uncertainty or equivocality". "Information. Data in context to inform or provide meaning for action".	DoD USA[132]	2014
"A basic unit of information built on standard structures having a unique meaning and distinct units or values".	DoD USA[133]	2015

Table 4.10. *Definitions of the term "data"*

130 DIKS: Data–Information–Knowledge–Wisdom

131 Harry D. Tunnell, "Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy", *Military Review*, pp. 43-50, May-June 2014, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20140630_art011.pdf.

132 DoD, Information Operations, JP 3-13, 20 November 2014, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

133 Joint Chiefs of Staff, Department of Defense, Dictionary of Military and Associated Terms, Joint-Publication 1-02, 8 November 2010 (as amended through 15 June 2015), 469 pages, United States, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Term	Definition
Metadata	"Metadata literally means "data about data." Metadata label, describe, or characterize other data and make it easier to retrieve, interpret, or use information"[134]. "Metadata is often called "data about data" and "is structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource"[135].
Data visualization	A discipline which consists of representing information in graphical form, communicating information in a form which is as easily comprehensible as possible.
Raw data	Data collected from a source, which have not undergone any treatment.
Big data	Massive data, large volumes of data, large datasets.
Open data	Digital data of public origin (i.e. produced by the State, government agencies, collectives, publicly–owned companies) or private origin, open to the public, made freely available.
Personal data	Data attached to individuals, which can be used to identify an individual.
Data–ism	Denotes the next phase in the evolution of the information society – that which is taking place right now, which has transformed data into the

134 Danette McGilvray, *Executing Data Quality Projects: Ten Steps to Quality Data and Trusted Information*, Morgan Kaufmann Publishers, 2008, http://booksite.elsevier.com/9780123743695/10steps_DataCategories.pdf.

135 European Parliament, Mass Surveillance, Science and Technology Options Assessment (STOA), PE 527.409, p. 102, December 2014, http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Annex%20Mass%20Surveillance%20Part%201.pdf.

	primary resource of the information economy. Data–ism is the title of a book by Steve Lohr[136].
Data at rest	Data which are inactive, stored, temporarily hosted on a system, as opposed to data flowing through the system. This formula is used in the domain of IT. It is also found in the US defense documents[137].

Table 4.11. *A number of concepts associated with that of "data" and their definitions*

4.3.2. *Some theories about data*

There are multiple characteristics which define data (sometimes used as a singular noun, representing a contiguous mass of data):

– data is a created object. Thus, it is the product of a process (of collection and treatment);

– data is a part of information, but does not constitute information when it is alone;

– data comes before information – in a manner of speaking, it is the raw material, the original prime material from which information is fashioned;

– the status of data can change: "data are increasingly closely interlinked, and increasingly disconnected from the documents in which they are reported"[138]. Thus, they acquire their own autonomy. On their own, though, data hold only very limited interest. In March 2009, at a TED conference, Tim Berners–Lee called for the creation of a web of linked data. In order to do this, it would be necessary to open up data, to allow links to form between these and other data and produce new knowledge and new correlations. "The web of the early

136 Steve Lohr, *Data-ism: the revolution transforming decision making, consumer behavior, and almost everything else*, Harper Business, 2015.

137 CJCSI 6510.F, Information Assurance and Support to Computer Network Defense, section C-49, p. 6, 9 February 2011, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf.

138 Manuel Lima, *Cartographie des réseaux : l'art de représenter la complexité*, Eyrolles, France, January 2013.

days, focused on documents, is giving way to a thriving ecosystem of data, a global data sphere where the main challenge (aside from issues of privacy) will be interoperability"[139]. "It is particularly interesting to see how the fundamental model of Internet autonomy has been replicated, exactly like in a fractal representation where the same principle of complexity and interconnections is applied to ever–finer parts of the structure: from routers to servers, and then to Web pages, and finally to data"[140];

– data is full of promise. With Big Data, there is even the question of a "radical transformation of society"[141], because the world is now controlled by data. Suffice it to say that data offers the prospect of a world where those in control of data – essentially data masses – hope to influence those who are not. The argument is certainly not a new one: the dawn of the Internet, of mobile telephony, its convergence toward the use of IP, and the emergence of social media also stirred up murmurings of radical social change, to cite only the most recent innovations (19th Century inventors too promised similar changes). "Through data, we can access opinions, feelings, behaviours, people, in real time, at great volume and at great speed. Tracking data is the Holy Grail. Data have the potential to transform all aspects of society, making all of its operations more efficient"[142]. The exploitation of data, life in a world immersed in data – a *datified world* – invite predictions of new evolutions for society, and, as is usually the case when new technologies emerge, the discourse oscillates between two approaches: one optimistic if not actually utopian, the other pessimistic if not actually catastrophist. For example, challenges arise in terms of power (economic, political) when that power is centered on data – i.e. the collection and exploitation thereof. Thus, does control of data differ from control of information, in terms of the conditions in which it takes place, its implementations and its goals?;

---

139 Manuel Lima, *Cartographie des réseaux: l'art de représenter la complexité*, Eyrolles, France, January 2013.

140 *Idem*.

141 Poetics and Politics of Data, Exhibition May-August 2015, Switzerland, http://www.hek.ch/en/program/events-en/event/poetics-and-politics-of-data.html.

142 Text of presentation from the "Data Power Conference", June 22-23, 2015, University of Sheffield, http://www.sheffield.ac.uk/socstudies/datapower.

– Barack Obama, during his presidential campaign in 2012, mobilized the capacities of big data to define his communication strategies[143]. Mathematical models appear to have been able to predict the results of the elections: "With the last set of polls factored into the model, my final prediction is Obama to win 332 electoral votes, with 206 for Romney" (November 6, 2012)[144]. That was the day of the elections, and almost all surveys carried out suggested Obama would win. The "predictions" of Drew Linzer (Assistant Professor of Political Science at Emory University) were confirmed by the election results: "The results are in: Obama wins all of his 2008 states, minus Indiana and North Carolina, for 332 electoral votes. This is exactly as I predicted on Tuesday morning – and as I've been predicting (albeit with greater uncertainty) since June" (November 9, 2012)[145]. The questions about the political role of data essential pertain to[146] the relation between data and surveillance/control; governance based on data; modes of resistance to data exploitation; regulation of the use of data, and of the actors involved; the role of data visualization in the political debate, etc.;

– data has a value: economic, strategic and political. In particular, it contributes to the mission of the actors in charge of national security. More broadly, it is a factor in power. It is at the heart of the national security strategies employed by the great nations[147], as attested by the surveillance programs some such countries have been running for decades;

143 Christy Wilson, Big Data in the Real World: Hadoop and the Power of Data in Politics, 7 August 2015, http://blog.syncsort.com/2015/08/big-data-in-the-real-world-hadoop-and-the-power-of-data-in-politics/.

144 Drew Linzer, Election day forecast: Obama 332, Romnay 206, November 6, 2012, http://votamatic.org/election-day-forecast-obama-332-romney-206/.

145 Drew Linzer, Final Result: Obama 332, Romnay 206, November 9, 2012, http://votamatic.org/final-result-obama-332-romney-206/.

146 "Data Power Conference", University of Sheffield, June 22-23, 2015, http://www.sheffield.ac.uk/socstudies/datapower.

147 Robert Beaton, Data science to the rescue, Future Force, 16 June 2014, http://futureforce.navylive.dodlive.mil/2014/06/data-science-to-the-rescue/

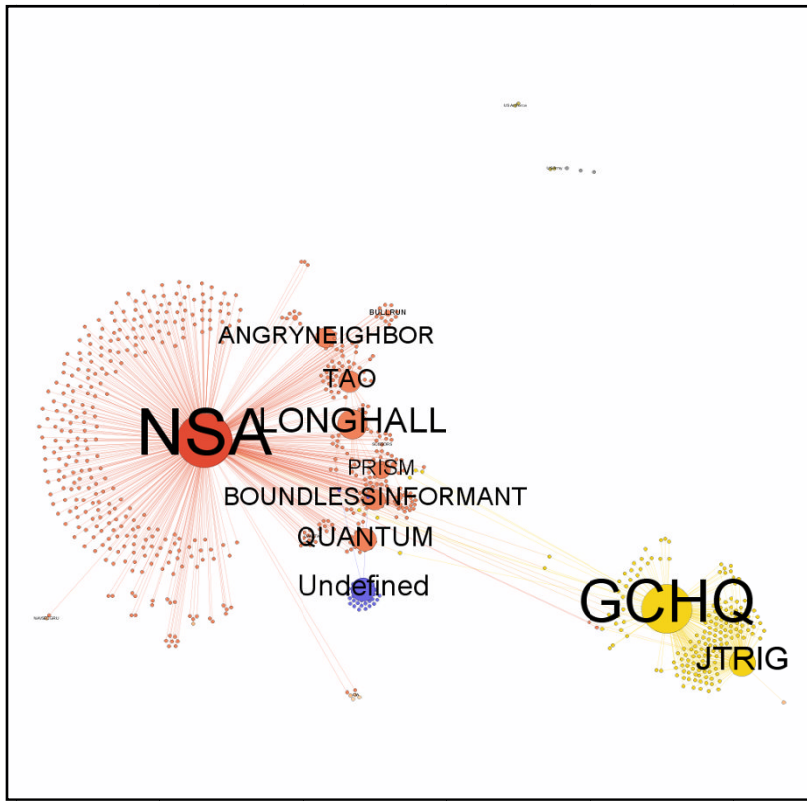


Figure 4.13. *The host of surveillance programs (mass data collection) deployed by the NSA and GCHQ (© Daniel Ventre 2015). For a color version of the figure, see www.iste.co.uk/ventre/warfare.zip*

– whilst data itself is not specifically vulnerable, its methods and supports of collection, processing, transmission and storage may be. The vulnerability of data contained and processed by computer systems, and the risks linked to the data for individuals, governments, armies and businesses are genuine problems, formulated as early as the 1960s, particularly in the works of Willis H. Ware – a researcher at the RAND Corporation: "Computer systems are now widely used in military and defense installations, and deliberate attempts to penetrate

such computer systems must be anticipated"[148]. "It should be clear, however, that access to files containing information about large numbers of people must be controlled"[149]. "Computer technology provides society with the tool it needs to accommodate growing information requirements. It lets us keep the records we have to keep, economically and efficiently. But the computer–based automated file can also work against us. The information in computer systems can be valuable and thus subverted for inappropriate purposes"[150]. Although the issue was observed even at that early stage, not a great deal appears to have been done to resolve it – we still face similar issues today, 40 years on. The data, and the actors who depend upon it, are faced with risks that the solutions (technical means, procedures, recommendations, laws) developed since then have not managed to solve. The phenomenon of massive data theft, and loss of databases (personal, industrial, commercial, secret, confidential, military data, etc.) is constantly feeding into cybersecurity statistics.

Incident	Country affected	Type of data	Origin	Date
Revelation of intrusions into the servers holding the databases of US Army personnel	United States	Personal data	China suspected	2015
Massive leak of personal data from the Japan Pension Service	Japan	Personal data		June 2015

148 Willis H. Ware, "Security and Privacy in Computer Systems", The Rand Corporation, Santa Monica, April 1967, http://www.rand.org/content/dam/rand/pubs/papers/2005/P3544.pdf.

149 Willis H. Ware, "The computer in your future", The Rand Corporation, Santa Monica, p. 50, November 1967, http://www.rand.org/content/dam/rand/pubs/papers/2008/P3626.pdf.

150 Willis H. Ware, "Data Banks, Privacy, and Society", The Rand Paper Series, Santa Monica, p. 17, November 1973: http://www.rand.org/content/dam/rand/pubs/papers/2008/P5131.pdf.

Hackers stole data of 1.25 million people[151]				
Benesse Holdings Inc. fell victim to data theft. The incident is believed to have cost the company 26 billion Yen[152]	Japan	Personal data		2014
Theft of the data of over 4000 Japan Airlines customers[153]	Japan	Personal data		2014
Theft of the bank details of 92408 Citigroup customers[154]	Japan	Personal data		2011
IRS Data Theft in the USA[155]	United States	Personal data	Russia	2015
Over 7 million usernames and passwords (stolen from the e–commerce sites on large Japanese companies) discovered on servers in Japan[156]	Japan	Personal data		2015

151 http://www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method/#.VdGt5_ntmko.
152 http://www.japantimes.co.jp/news/2015/05/01/business/corporate-business/benesse-posts-first-group-net-loss-in-wake-of-massive-data-theft/#.VdGwq_ntmko.
153 https://www.jal.co.jp/en/info/other/140924.html.
154 http://www.wsj.com/articles/SB10001424053111903366504576490541082030476.
155 http://www.huffingtonpost.com/harlan-green/the-irs-data-theft-and-pu_b_7464490.html.
156 http://www.databreaches.net/7-85-million-ids-passwords-found-on-seized-proxy-servers-in-japan/.

Large-scale data theft from the company Hacking Team (which sells surveillance solutions): lists of the company's clients, financial data, etc.[157]	Italy	Personal, contractual, commercial, industrial (etc.) data		2015
Data theft from the servers of the company MSpy (which provides spyware)	UK	Personal data, commercial data, etc.		2015
Theft of the data of 150 million eBay users	USA			2014
The data of 102 million customers of the platform Sony Online Entertainment Services were exposed.				2011
Theft of social security numbers of US Army veterans	United States			2008
Office of Personnel Management	United States			2015

Table 4.12. *Various attacks on databases*

– data can be used to construct a space, a specific environment, which feeds into or precedes the information space. We shall use the metaphors "data universe" or "data halo", to which, in any case, the various data representations or visualizations typically refer;

157 http://www.zdnet.com/article/hacking-team-data-theft-culprit-exposed/.

– the Balkanization of data storage systems[158] refers to the geographical and organizational decentralization of data centers – a state of affairs which increases the number of operations carried out on the volumes of data (extractions, transfers, etc.). The metaphor also refers to the idea of sovereignty (over the data, but also over the systems, the technology, the parcels of cyberspace), defined as "different state behaviours towards data generated in or passing through national internet infrastructure"[159]. The United States and their allies consider that localizing data (attaching it to a territory) constitutes a threat to the freedom of flows in cyberspace; Russia and China, for their part, are proponents of a sovereign approach, aiming to protect sensitive, national data from prying foreign eyes. "Data sovereignty refers specifically to the attempt by nation–states to subject data flows to national jurisdictions"[160]. Thus, the different approaches pertaining to the status of data are at the heart of the international disagreements. The question of data sovereignty is merely one element of the broader issue of cyberspace sovereignty and the Balkanization/fragmentation of cyberspace into national spaces[161].

4.3.3. *Visualization*

The Internet offers us increasing numbers of online applications and data visualization platforms. There are numerous industries – not just security industries – developing such applications.

158 Christos Karamanolis, On the Balkanization of data storage, VMware, 5 January 2015: https://blogs.vmware.com/cto/balkanization/.

159 Dana Polatin-Reuben, Joss Wright, An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet, p. 10, 7 July 2014, https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf.

160 Dana Polatin-Reuben, Joss Wright, An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet, p. 10, 7 July 2014, https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf.

161 Jonah Force Hill, Internet Fragmentation Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers, John F. Kennedy School of Government, Harvard University, p. 52, Spring 2012, http://belfercenter.ksg.harvard.edu/files/internet_fragmentation_jonah_hill.pdf.

"The representations of the data may be beautiful, elegant and descriptive"[162]. Growing numbers of software tools, growing platforms from multiple sources, enable us to visualize masses of data, via interfaces where esthetics disputes usefulness. Now dynamic Websites are able to display real–time data, in the form of animations and/or tables showing data (e.g. mashup on the city of London). Static maps and maps/images produced by software, sometimes handling vast quantities of data, were supplanted a few years ago (in the 2000s) by the new possibilities for dynamic representations. Various types of content – particularly data streams – are the object of real-time visualizations: the flow of air traffic, marine traffic, road networks, evolution of the blogosphere, etc.

	Content
Norse IPVicking Live	Cyber attacks
Digital Attack Map (Google)[163]	DDoS attacks
Logbook[164] targeted cyber attacks	APT
Akamai Real Time Monitor[165]	Cyber attacks
F–Secure Glob[166]	Malware
Kaspersky Cyberthreat Real–Time Map[167]	Cyber threats
Deutschen Telekom[168]	Cyber attacks

162 Vitaly Friedman, Data Visualization: Modern Approaches, 2 August 2007: http://www.smashingmagazine.com/2007/08/02/data-visualization-modern-approaches/.
163 http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=15999&view=map.
164 https://apt.securelist.com/#firstPage.
165 http://www.akamai.com/html/technology/dataviz1.html?WT.ac=hp_attacks.
166 http://globe.f-secure.com/.
167 http://cybermap.kaspersky.com/.
168 http://sicherheitstacho.eu/.

ThreatMetrix[169]	Cyber crime attacks
CIRCL Map[170]	Cyber attacks
Honeynet Project[171]	Cyber threats
FireEye Cyber Threat Map[172]	Cyber threats
CISCO[173]	Global cyber threat
Trend Micro[174]	Botnet infection
Trend Micro[175]	Spam
Atlas – Arbor Networks[176]	Cyber attacks, phishing, botnets
AlienVault. Global Threat Dashboard[177]	Spam
Securitywizardry[178]	Cyber Threat Intelligence
Tweetping[179]	Visualizing tweets live
Globetweeter[180]	Visualizing tweets all over the world
Tag Galaxy[181]	Visualizing tags using Flickr data

169 http://www.threatmetrix.com/threatmetrix-labs/web-fraud-map/.
170 http://map.circl.lu/.
171 http://map.honeynet.org/.
172 https://www.fireeye.com/cyber-map/threat-map.html.
173 https://labs.opendns.com/global-network/.
174 http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-botnet-map/index.html?ClickID=cfzfzzpannwl7qwi4lkpizivaqve44feqkz.
175 http://www.trendmicro.com/us/security-intelligence/current-threat-activity/global-spam-map/index.html.
176 http://atlas.arbor.net/worldmap/index.
177 https://www.alienvault.com/open-threat-exchange/dashboard#/threats/recent.
178 http://www.securitywizardry.com/radar.htm.
179 http://tweetping.net/.
180 http://plopbyte.com/globetweeter/.
181 http://www.taggalaxy.de/.

Cartodb[182]	The activity of major cities
Earth[183]	Currents of air masses all over the globe
Flighttracking[184]	The activity of Luton Airport (UK)
Marinetraffic[185]	Maritime traffic
Flightradar[186]	Real-time airspace throughout the world
AGICN[187]	Air pollution
Radioactiveathome[188]	Map of radioactive zones
Submarinecablemap[189]	Interactive map of submarine Internet cables
LivePlasma[190]	Creates connections between artists and films

Table 4.13. *Data visualization tools*[191]

In the field of cybersecurity, the representation of data has become extremely important in recent years, by the combined effect of the increase in number of data sources, improved collection capabilities,

182 http://cartodb.pr.co/51479-here-and-cartodb-partner-to-visualize-24hrs-of-life-in-cities.
183 http://earth.nullschool.net/#current/wind/surface/level/orthographic=-213.95,15.64,690.
184 http://www.london-luton.co.uk/en/flighttracking/.
185 https://www.marinetraffic.com/fr/.
186 http://www.flightradar24.com/48.01,7.5/9.
187 http://aqicn.org/map/.
188 http://radioactiveathome.org/map/.
189 http://www.submarinecablemap.com/#/landing-point/fuzhou-china.
190 http://www.liveplasma.com/.
191 Various sites have lists of the various visualization platforms, interactive or otherwise, that can be used to process data – notably exploiting data from the Web (blogs, tweets, feeds, etc.). For instance, see http://www.webdesignerdepot.com/2009/06/50-great-examples-of-data-visualization/.

and better processing systems (big data), but also the new-found importance of cybersecurity issues and the need to better understand the phenomena at play. Visualization is guided by a utilitarian need: to be able to quickly see, in real time, what is happening on the networks of a business, an administration, or on larger-scale networks, such as the blogosphere.

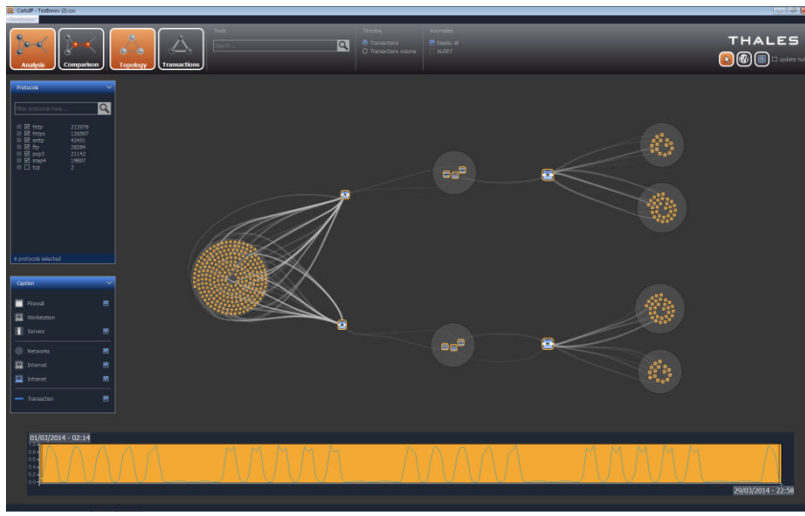


Figure 4.14. *The CYBELS–MAP application developed by Thales. Graphical representations of exchanges between networks – e.g. a business network and the outside world. Each dot represents a machine or an IP address. © THALES. For a color version of the figure, see www.iste.co.uk/ventre/warfare.zip*

Real-time visualization of cyber attacks has become possible because of platforms whose visual results are, to say the least, spectacular: with the ambition of offering a real-time view of all the events (incidents) across the whole of the planet, these representations convey the image of a world of constant and global insecurity. Indeed, there are no regions of the world which appear to be spared the phenomenon.

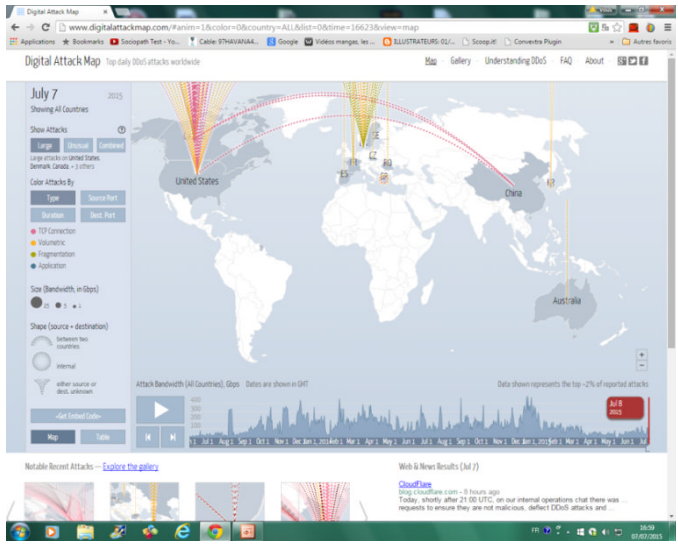


Figure 4.15. *Visualization of cyber attacks, confirming or giving the impression of a conflict between China and the United States. Source: screenshot from the application Digital Attack Map. 7 July 2015. For a color version of the figure, see www.iste.co.uk/ventre/warfare.zip*

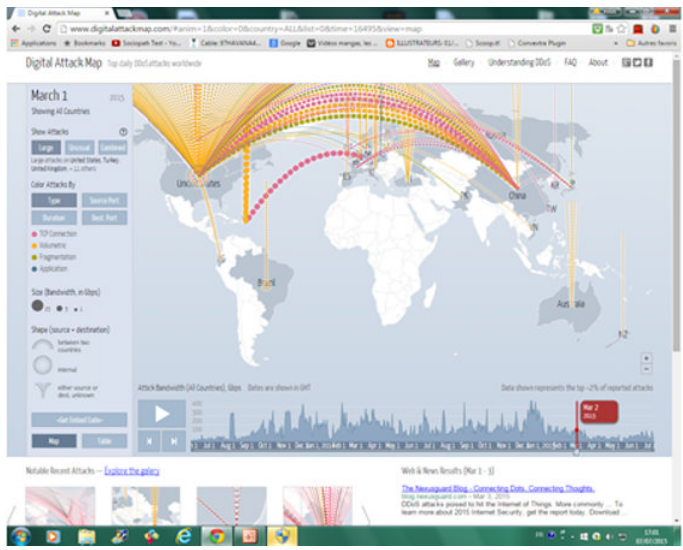


Figure 4.16. *Screenshot from Digital Attack Map, 1 March 2015. For a color version of the figure, see www.iste.co.uk/ventre/warfare.zip*

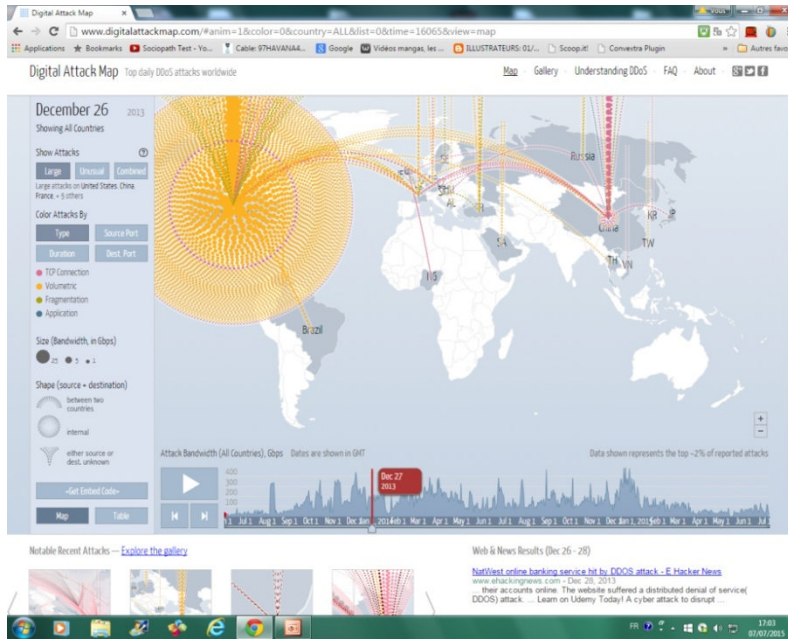


Figure 4.17. *Screenshot from Digital Attack Map, 26 December 2014. For a color version of the figure, see www.iste.co.uk/ventre/warfare.zip*

These observations invite a number of critical comments:

– the purpose of data visualization (with a view to transforming data into information) is to modify points of view, to be able to view the world differently, to render it more legible and comprehensible, and partly overcome the *complexity* of a global system. Big data and the tools of data visualization and data analytics should enable us to manage, view and analyze a complex system, simplify it, reduce it and exploit it, by revealing its hidden rules. A complex system is any which includes a large number of variables (multi-variable approach), connected to one another, and mutually interdependent (e.g. the SI international system, a neural network, a social network, the Internet, and so on);

– the modes of representation are not impartial. They give rise to certain effects by influencing perception, understanding and analysis.

Our understanding and our reading of the world are altered by maps, the forms they take, the ways in which we can or cannot interact with them, how we can or cannot select data and act upon them. What we see determines our interpretation of the environment. Through these maps of the world showing cyber attacks, our image of a world is constructed or reinforced: the image of a cyber–environment dominated by the superpowers (the attack paths usually massively join North America with Asia or Europe). However, states shown to be exchanging cyber attacks are not necessarily at war. Yet the observer is left with that impression: that he/she is witnessing a confrontation – a major conflict. Sources and targets do not always appear to be clearly distinguished. Their identities are not known. The nature of the incidents tends to be forgotten, and the lines arcing from one point to another resemble the trajectories of missiles launched by one state against another. Being unaware of the parties' identities, the impacts, the subtle nuances which may be contained in the source data but smoothed out by the visualization, the observer sees a world victim to phenomena s/he is informed are "attacks". Thus, the representations are partial, imperfect instruments of influence. Above all, it is important to avoid drawing hasty conclusions about the ratio of strength between states, especially as this is an entirely separate issue;

– besides the limitation of screen size, other factors directly impact the quality of representations: the quality of the source data, of the sensors, of the treatment algorithms, the computational power, and the representation codes chosen. The majority of representations are not sufficient in themselves. The very complexity of the phenomena they are intended to express necessitates the support of an explanatory text, sometimes lengthy explanations, decryption and an expert opinion;

– the person who reads or views the information, delivered to him/her in the form of images, is usually unaware of the origin and nature of the data, and the nature of the treatment those data have undergone. The danger is that an esthetically-pleasing presentation can mask inadequacies in terms of the quality of the data and the treatment thereof. There is also a risk of manipulation, of deliberate misrepresentation of a reality by inappropriate processing of the data

(even if only because there are insufficient numbers of sensors to hope to represent the real situation in its entirety, for example).

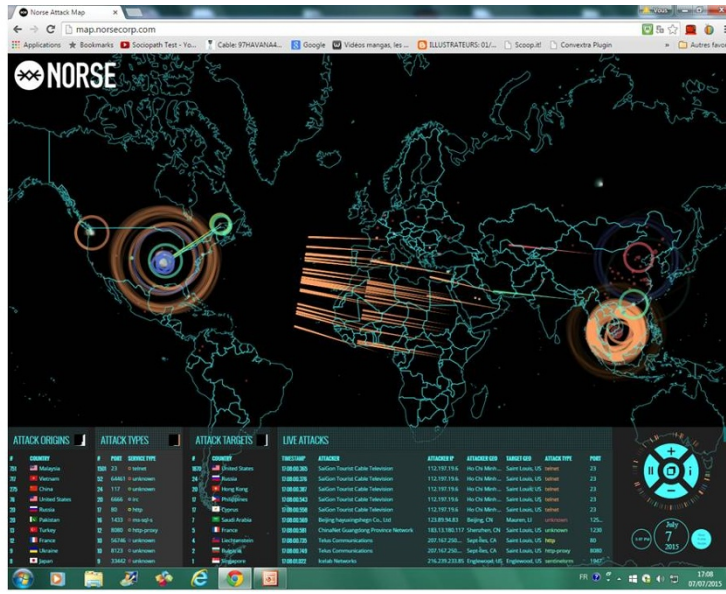


Figure 4.18. *Screenshot from the online application Norse, 7 July 2015. For a color version of the figure, see www.iste.co.uk/ventre/warfare.zip*

Visualizations based on geographic maps present the following information (whether or not in real time):

– geographic locations (country);

– identified source of an attack (but not necessarily its true source);

– identified target of an attack (but not necessarily the target actually struck at);

– intensity, volume (expressed by choice of colors, animations);

– nature of the attack (animated maps generally focus on a single type of attacks – e.g. DDoS. They are not exhaustive, cannot represent everything or express every aspect of the state of insecurity or security, violence, etc.).

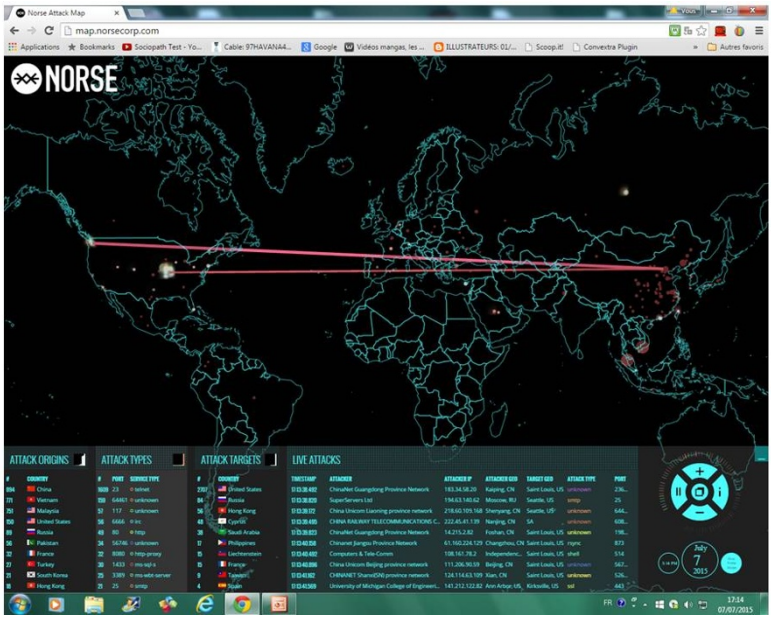


Figure 4.19. *Screenshot from the online application Norse.7 July 2015. For a color version of the figure, see www.iste.co.uk/ventre/warfare.zip*

These representations cannot integrate pertinent information, which is critical for the analysis of the strength ratios:

– the identity of the actors (sources, targets). The crude geographical localization means it is impossible to speak of identity. The very notion of identity is reduced to that approximate geographical location;

– the duration of the attacks;

– the reactions;

– the effects produced;

– the "normal" or "exceptional" nature of the situation at time *t*. A visualization focused on one instant cannot offer a long–term perspective, provide means of comparison or contextualization.

4.3.4. *Data warfare?*

4.3.4.1. *Data in military doctrine*

The defense forces, whether in operation or not operation, are producing ever increasing volumes of data. The vast masses of data produced are characteristic of modern combat operations[192].

Defense approaches distinguish between data and information, and thus between mastery/exploitation of data and information. As is the case with information, we can anticipate a defensive and offensive perspective, and the involvement of data in armed conflicts. Here, we shall focus on the overlaps or divergences between the three objects which are information, data and cyber. Information and cyber have been modeled in terms of spaces (information space or information environment, and cyberspace). Does data lend itself to a spatial model? In addition, whilst information and cyber have given rise to information warfare (and infowar) and cyber warfare (in the official vocabulary, preference is given to cyber security, cyber defense, cyber attacks or cyber conflict), can data be used to construct "data warfare"? Taking account of information and cyberspace in the forces has resulted in the creation of dedicated units, specialized professional areas, a specific hierarchical organization (information warfare units in armies – which has since become information operations units; cyberdefense units, and the creation of institutions such as the US cyber command), but will taking account of the specific role of data redefine the boundaries of these structures devoted to information and cyber, lead to the establishment of new units, strategies and additional doctrines? Are we going to see the emergence of complementary aspects or competitions between information operations, cyberdefense and data warfare?

The US Department of Defense Dictionary[193] defines data as follows: "1. A basic unit of information built on standard structures

192 Harry D. Tunnell, Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy, Military Review, pp. 43-50, May-June 2014, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20140630_art011.pdf.

having a unique meaning and distinct units or values. 2. In electronic recordkeeping, a combination of characters or bytes referring to one separate item of information, such as name, address, or age"[194]. Below, we list all of the subdivisions of data appearing in that official document:

– data: antemortem data, authorization data, restricted data category, geospatial–intelligence data, statistical data, geodetic data, toponymic data, status data, health-related data, positional data, Integrated Data Environment, electronic data, data repository, data center, data processing, meteorological and oceanographic data, movement data, force and deployment data, raw data, numerical data, tactical data link, personnel data, movement data, data elements, automated data processing, accident data recorder, authoritative data source, analog simple data interface, Advanced Tactical Data Link System, airborne tactical data system, basic identity data element, Advanced Field Artillery Tactical Data System, common data link management system, continuous data recording, commercial electronic data interface, Combined Information Data Network Exchange, data adapter aerospace drift, data administrator, data adapter control block, data adapter control mode, data adapter termination unit, data collection device, data channel multiplexer, data distribution center, digital data link, digital data modem, data integration and exploitation, Deployable Intelligence Data Handling System, defense information threat data system, defense intelligence threat data system, defense management data center, defense manpower data center, data manipulation language, data orderwire, data patch panel, digital terrain elevation data, data collection plan, electronic data interchange, emitter locating data, flight data recorder, high speed serial data buffer, intelligence cutoff data, Intelligence Data Elements Authorized Standards, imagery data, Integrated Data Environment, joint data network, Joint Resource Assessment Data System, joint track data coordinator, military information support

193 Joint Chiefs of Staff, Department of Defense, Dictionary of Military and Associated Terms, Joint-Publication 1-02, 8 November 2010 (as amended through 15 June 2015), 469 pages, United States, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
194 Page 59.

operations automated data system, migration defense intelligence threat data system, Modernized Defense Intelligence Threat Data System, meteorological data system, multi–tactical data link network, Naval Oceanographic Data Distribution System, naval tactical data system, positional data graphic, Reserve Component common personnel data system, situation awareness data link, surveillance control data link, satellite data link standards, signals external data, tactical operational data, transmit data, tactical data link, tactical data network, technical operational data, Table Formatted Aeronautic Data Set, tactical ocean data, tactical terrain data, unit movement data, vessel arrival data;

– database: intelligence database, planning factors database, air operations database, consolidated counterdrug database, combating terrorism database, database administrator, digital bathymetric database, database generation, database management system, digital point positioning database, defense sexual assault incident database, explosive hazard database, functional database manager, integrated database, modernized integrated database, modernized intelligence database, naval intelligence database, planning and execution database, planning factors database, point positioning database, Satellite Communications Database, technical database management, user requirements database;

– enumeration of data-centered entities and defense structures: Allied Data Systems Interoperability Agency (ADSIA); European Data Analysis Center; Data Information Coordination Office (DICO); National Climatic Data Center; National Environmental Satellite, Data and Information Service; Defense Manpower Data Center.

The concept of information[195] is not defined in that dictionary. The DoD draws a distinction between "data" and "information" (data is "a basic unit of information"). This distinction is manifested in many entries in the dictionary: "statistical data and information"[196] or

195 The term "information" appears 645 times in the dictionary (2015 version), as compared to 242 occurrences of the term "data".
196 Page 97.

"information management [is] the function of managing an organization's information resources for the handling of data and information acquired by one or many different systems, individuals, and organizations in a way that optimizes access by all who have a share in that data or a right to that information"[197]; "technical intelligence [is] intelligence derived from the collection, processing, analysis, and exploitation of data and information". Data is the raw material which then needs to be processed and analysed to be transformed into information: "processing [is] a system of operations designed to convert raw data into useful information"[198].

The idea of information is associated with the following expressions, defined in the dictionary: information assurance; information environment[199]; information management; information operations[200]; information operations force; information operations intelligence integration; information-related capability; information report; information requirements; information superiority.

Information operations are offensive and defensive operations conducted by the military (information operations force), employing specific capabilities (information-related capabilities, intelligence, deception, information assurance, etc.)[201], in an information environment where we find more than just military personnel (because the definition tells us that the information environment is an aggregate of individuals and organizations, and is not limited to the military domain), which are targeted at adversaries (and potential adversaries)

197 Page 112.
198 Page 193.
199 "The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (JP 3-13)".
200 "The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO. See also electronic warfare; military deception; operations security; military information support operations (JP 3-13)".
201 The full list of operations and capabilities involved in information operations is not given in that document.

whose decision–making processes we wish to influence or impede, and over which we wish to have informational superiority[202].

The term "cyber", for its part, arises 43 times in the document, giving root to:

– cyberspace: cyberspace operations, defensive cyberspace operations, passive and active cyberspace operations, offensive cyberspace operations; cyberspace superiority; cyberspace capabilities, friendly cyberspace capabilities; cyberspace support element; joint cyberspace center; NMS–CO (National Military Strategy for Cyberspace Operations); cyberspace attack;

– cybersecurity: Comprehensive National Cybersecurity Initiative (CNCI), National Cyber Security Division (NCSD);

– enumeration of entities and units focusing on cyber matters: CDRUSCYBERCOM (Commander, United States Cyber Command); COMFLTCYBERCOM (Commander, Fleet Cyber Command); DC3 (Department of Defense Cyber Crime Center); FLTCYBERCOM (Fleet Cyber Command – Navy); NAVCYBERFOR (Navy Cyber Forces); NCIJTF–AG (National Cyber Investigative Joint Task Force–Analytical Group – DOD); NCRCG (National Cyber Response Coordination Group); USCYBERCOM (United States Cyber Command).

"Cyberspace operations" are defensive[203] and offensive operations ("the employment of cyberspace capabilities), carried out in cyberspace ("a global domain within the information environment"[204]) to achieve objectives (the dictionary does not specify these further[205]),

202 "[I]nformation superiority – The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. See also information operations (JP 3-13)".
203 Page 63.
204 Page 58.
205 "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace".

such as superiority (which, for its part, is inarguably a military goal)[206].

Cyberspace, as defined in this dictionary, is the space in which data flow: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data". The definition of defensive operations also makes reference to data: "defensive cyberspace operations – Passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems"[207].

Yet cyberspace is also the arena of information, because the definition of cybersecurity integrates the concept of information rather than data: "cybersecurity [is] prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (DODI 8500.01)".

The "Joint Intelligence" document published on 22 Octeber 2013 (Joint Publication 2–0) 208 from the US Department of Defense, published by the CJCS, describes the relations between data, information and intelligence: "Raw data by itself has relatively limited utility. However, when data is collected from a sensor and processed into an intelligible form, it becomes information and gains greater utility. Information on its own may be of utility to the commander, but when related to other information about the OE and considered in the light of past experience, it gives rise to a new understanding of the information, which may be termed "intelligence"[209].

206 "Cyberspace Superiority – The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force, and its related land, air, maritime, and space forces at a given time and place without prohibitive interference by an adversary", page 58.
207 Page 63.
208 http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.
209 Page I-1.

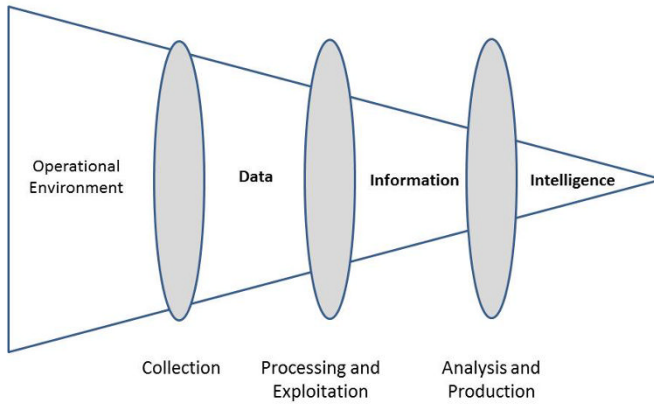


Figure 4.20. *Data–information–intelligence relationship. From a diagram published in JP–02 (2013).*[210] *The Canadian Air Force doctrine from 2012*[211] *adds a further stage – understanding – to construct a cognitive hierarchy linking data, information, intelligence and understanding. Data, which are always at the base of the pyramid, becomes knowledge after a set of treatment processes*

The standards defined by the DISA, pertaining to the transfer of data to the Cloud, propose three categories of data. Armies transfer their data to the Cloud, driven by economic imperatives (reducing costs) and security concerns[212]. The objective is to distribute data within the American defensive forces, via a cloud that is specific just to them. The Defense agencies, though, have been authorized to use private solutions (in December 2014)[213], rather than only those of the

210 Joint Publication 2-0, Joint Intelligence, October 2013: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf.

211 http://airforceapp.forces.gc.ca/cfawc/CDD/Doctrine/Pubs/Operational/402_Series/B-GA-402-000-FP-001.pdf.

212 Cheryl Pellerin, DoD Moves Data to the Cloud to Lower Costs, Improve Security, DoD News, Defense Media Activity, Washington, 30 January 2015: http://www.defense.gov/news/newsarticle.aspx?id=128083.

213 Department of Defense, Chief Information Officer, Washington, Memorandum for the secretaries of the military departments, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, p. 4, December 15, 2014, http://iase.disa.mil/Documents/commercial_cloud_computing_services.pdf.

DISA (abandonment of the "DISA first" strategy)[214]. However, to ensure that these partnerships with the private sector are not a source of insecurity, rules are defined, DISA monitors the choices made, and data have been classified into 3 categories (initially 6).

Category	Type of data, rules
1–2	"Data lives in the commercial cloud. Not requiring physical separation or access to DoD network – information is fully public or discoverable through FOIA requests".
3–4	"More sensitive business systems that support operations of the department. Data will be separated into a virtual cloud environment that will require a secure connection to DoD networks".
5–6	"National security systems will exist in a physically separate environment not connected to a virtually accessible cloud".

Table 4.14. *The three categories of data and the rules pertaining to them. The texts cited above are extracted from Aaron Boyd, 2015*[215]

In America's JP 2–0, the concept of data is divided into multiple items: database, raw data, force and deployment data, collected data, data conversion, data correlation, meteorological and oceanographic data, quantitative data, biometric, biographic, forensic, and DOMEX data, archived data, relevant/irrelevant data, required data, data formats, imagery data, Electromagnetic data, Radar data, Radio frequency data, Geophysical data, Materials data, Nuclear radiation data, statistical data, geodetic data, institutional data, contextual data, biologic identity data.

214 http://www.datacenterknowledge.com/archives/2015/02/05/department-of-defense-works-with-commercial-cloud-providers/.

215 Aaron Boyd, New DoD cloud security requirements coming Tuesday, Federal Times, January 13, 2015: http://www.federaltimes.com/story/government/cybersecurity/2015/01/12/dod-cloud-security-guidance/21653107/.

The concepts of big data, open data and metadata are absent from the report. The concept of "cyber" is absent from the document. That of information is omnipresent, and once again it speaks about the information environment, which is described as being made up of three dimensions: the "physical, informational, and cognitive dimensions"[216].

Data are also the subject of the document *Information Operations (JP 3–13)* published on 27 November 2012, and modified on 20 November 2014[217]. The document offers a representation of the information environment, which is still constructed around three elements. The information dimension is said to be "data-centered".

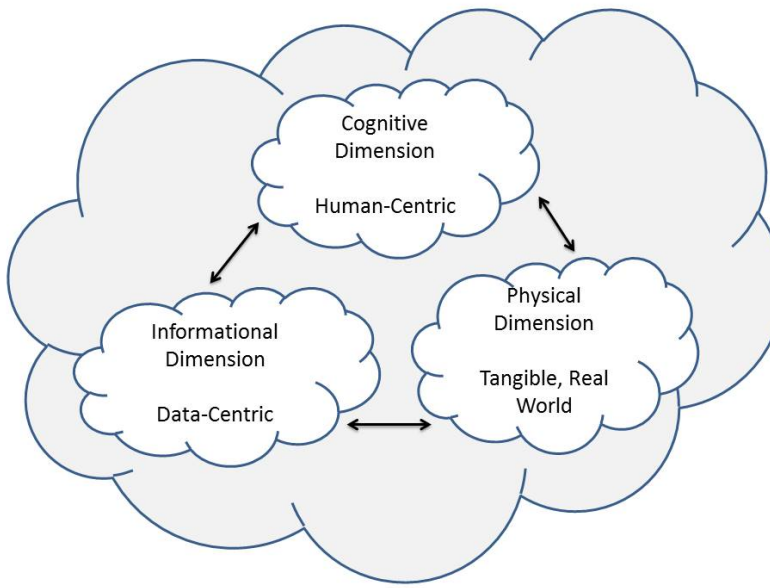


Figure 4.21. *The information environment, as defined by JP 3–13 in November 2014*

216 Page I-27.
217 http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

The three elements of the data–information–knowledge continuum are thus defined[218]:

– "data. Interpreted signals that can reduce uncertainty or equivocality";

– "information. Data in context to inform or provide meaning for action";

– "knowledge. Information in context to enable direct action".

The Canadian Air Force doctrine of 2012[219] also sheds light on the way in which the military deal with data.

Data, alongside information and knowledge (that well-known trio) is essential to the mastery of the operational environment. These three elements need networks and cyberspace, in order to be created, collected and disseminated. Everything (networks, cyberspace, data, information and knowledge) falls within the information domain. The text mentions the necessary fusion of data and information, with the objective being to produce information which is accurate, secure and provide a coherent vision. We must undoubtedly understand the fusion of data and information to be the implementation of a process where the information is based on quality data (there can be no useful, reliable information without reliable data). In the Canadian Air Forces, the "sense" function lies in the delivery of knowledge, integrating all the processes from data collection to production of that knowledge. Thus, the report describes what it calls "cognitive hierarchy" – a succession of processes which, starting with data, apply treatments to transform it into information, which must, in turn, become knowledge, which will, in the final stage of the string of

218 On this subject, the following publication is also recommended reading: Harry D. Tunnell, Network-Centric Warfare and the Data-Information-Knowledge-Wisdom Hierarchy, Military Review, pp.43-50, May-June 2014, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20140630_art011.pdf.

219 Canadian Forces Aerospace Sense Doctrine B-GA-402-000/FP-001 Commander of the Royal Canadian Air Force, p. 66, August 2012, http://airforceapp.forces.gc.ca/cfawc/CDD/Doctrine/Pubs/Operational/402_Series/B-GA-402-000-FP-001.pdf.

processes, become useful for decision-making (understanding, decision). Mere possession of the data has no tactical, operational or strategic value. Thus, not all data can be collected. Data collection must be thought of as a function of the purpose of the series of processes (no knowledge or understanding can be reached if the data are not useful).

Three types of data need to be collected (information and knowledge then to be produced): those pertaining to the enemy, those concerning one's own allies, and those regarding third parties, with the ensemble offering an overall understanding of the operational environment of the forces. Data processing, action on the data, consists of: collecting, organizing, prioritizing, filtering, analyzing, sorting, focusing, fusing, confirming, validating, formatting, storing, disseminating, etc. Data results from the observation and measurement of the physical world. One of the major challenges lies in the enormous quantity of data, which grows phenomenally over the course of the operations, and can render the exercise of command (decision–making) difficilt. Data also need to be reusable: "it is prudent to manage data under the principle of 'enter data once, use many times'"[220].

There again, information is only the second layer. Data is fundamental: it is the base of the pyramid. However, the majority of doctrines and theories or strategies, in Canada and indeed everywhere, focus on information as a whole, an absolute (to be mastery, dominated, on which to act, from which everything stems and towards which everything converges). The dedicated formulas are "information warfare", "information operations", "information superiority" and "information dominance"; mention is even made, sometimes, of "knowledge warfare"; but there has been no question of data warfare, conflict for data or conflict in a data space, a data environment.

220 Page 15.

Document	Comment, analysis
Strategy pertaining to data	
DoDD 8530.1 CND	
DoD Net–Centric Data Strategy[221] 9 May 2003	The data in question here are those which feed into network-centric operations. The aim is to define the modes and principles of data management in a network-centered defense environment. The key principles are as follows: – data must be rendered accessible and be shared as widely as possible (except for data which are subject to restrictions, such as security data, which are sensitive and classified); – data must be useful for the decision-making processes. However, as we cannot *a priori* decide which on data will be useful, the principle is to offer all the data, and then allow the functions/ missions/professionals/users deal with the data to render them useful for their own objectives. We must provide the data without waiting for them to have undergone treatment. They will be processed by those people who decide upon them and have need of them. (This is the idea behind "data as a service" – DaaS). The logic differs from that which was previously in force, substituting the principle of "process, exploit, and disseminate". The principle is now formulated as "*post before processing*". This logic involves organization changes, but also cultural ones (who has power other the data?); – as data must be exploitable and searchable, it is useful for them to by *tagged with metadata*; – data are made available to "*communities of interest* – COIs" (an expression denoting groups of users sharing objectives, interests, goals, etc.).
DoD Data strategy[222] 2007	Article. Interview given by Michael E. Krieger, Director for information policy at the DoD.

221 DoD Net-Centric Strategy, Department of Defense, Washington, 9 May 2003, 30 pages: http://dodcio.defense.gov/Portals/0/Documents/DIEA/Net-Centric-Data-Strategy-2003-05-092.pdf.
222 Michael E. Krieger, Data Strategy at the Department of Defense, CIO, 4 October 2007: http://www.cio.com/article/2437949/service-oriented-architecture/data-strategy-at-the-department-of-defense.html.

	Vulnerabilities: "Our weakness is that we build systems that are too tightly coupled to the data". *Data as a service*[223]: The new approach to data security is based on the following principle: "data is available as a service, and applications are independent of the data". *Metadata*: The standards used by the defense may be the same as those used in industry: "We didn't make up our metadata standard. The DDMS[224] is based on the industry Dublin Core standard".
Data and DISA (in particular, see the concept of "elastic data environment") 2009[225]	This document introduces the concept of an "elastic data environment" to denote an "environment where compute and storage capacity is flexible, interoperable, and transient".
Marine Corps Data Strategy[226] Department of the Navy, MCO 5231.3, 7 April 2009	This document defines the "policy for data production, data storage and data replication, data/information exchange, participation in NCDS Communities of Interest (COIs), registration of Authoritative Data Sources (ADS), and database registration". The need to share data is tempered by the need to protect them. The requirements of net–centric operations will be respected provided that they do not endanger the security of the marines.
Army Data Strategy. 19 December 2011[227]	Implements the DoD Data Strategy
Instruction[228] Sharing Data, Information, and	3 categories of "services" are identified: Data, information, and IT services. These services must be

223 Exposing Data as a Service in the Army Enterprise , MIT Information Quality Industry Symposium, p. 17, July 15-17, 2009, http://mitiq.mit.edu/IQIS/Documents/CDOIQS_200977/Papers/03_02_3A-2.pdf.
224 Department of Defense Discovery Metadata Specification (DDMS).
225 DISA Strategic Plan 2015 – 2020, 6 October 2015, 16 pages: http://www.disa.mil/~/media/Files/DISA/About/Strategic-Plan.pdf.
226 Marine Corps data strategy, Order 5231.3, Department of the Navy, 7 April 2009, 14 pages: http://www.marines.mil/Portals/59/Publications/MCO%205231.3.pdf.
227 US Army, Chief Information Officer, Army Data Strategy, 19 December 2011, 1 page, http://ciog6.army.mil/Portals/1/InfoSheet/04-ADS_Info%20Paper%20(1p)_v1.pdf.
228 Reissues DoD Directive (DoDD) 8320.02 (Reference (a)) as a DoD Instruction (DoDI) http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf.

Information Technology (IT) Services in the Department of Defense. no. 8320.02. August 5, 2013	interoperable, secure and accessible. Their standards are specified in the DoD IT Standards Registry (DISR).
DoD strategy for defending networks, Systems, and Data, 13 November 2013[229]	– Increasing the use of Big Data ("Big Data analytics is the process of examining very large amounts of data to uncover hidden patterns, unknown correlations, and other useful information". – Strengthening the defense of data by ensuring confidentiality and integrity of the data throughout its lifecycle.
Cloud Computing	
Marine Corps cloud computing strategy, 15 May 2012[230]	The Marine Corps is implementing a private cloud computing environment (PCCE).
DoD Memorandum, "Designation of the Defense Information Systems Agency as the Department of Defense Enterprise Cloud Service Broker" (canceled) June 26, 2012	Charges the agency of supplying cloud computing services and infrastructures to the DoD.
Cloud for defense challenge	– ever–increasing numbers of users (a million military personnel use the DOD Enterprise Email – DEE[231]. – data security. – the technological transition itself (constructing the cloud architecture within the forces).
Potential applications	– Cyber Network Defense, Battlespace Awareness,

229 Department of Defense, Chief Information Officer , DoD Strategy for Defending Networks, Systems, and Data, 13 November 2013, Washington, 8 pages, http://iac.dtic.mil/csiac/download/DDNSD_Public_Releasable_11132014.pdf.
230 Marine Corps Private Cloud Computing Environment Strategy, 15 May 2012, 16 pages, http://www.hqmc.marines.mil/Portals/156/Newsfeeds/SV%20Documents/Marine_Corps_Private_Cloud_Computing_Environment_Strategy_15_May_2012.pdf.
231 Bill Kleyman, DoD Cloud Adoption Helps U.S. troops stay connected, 24 May 2013: http://www.datacenterknowledge.com/archives/2013/05/24/dods-cloud-adoption-helps-troops-connect/.

	Simulation and Visualization, "corporate/business" applications[232].
Department of Defense, Chief Information Officer, Washington, Memorandum for the secretaries of the military departments, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services.[233] December 15, 2014	The obligation to use DISA's services has been relaxed. The defense components retain a greater degree of freedom in the choice of cloud computing providers and solutions[234].
US Army cloud strategy[235], March 2015	The cloud infrastructure is essential for the creation of the Joint Information Environment (JIE). Whilst the DoD cannot forgo these cloud architectures in its effort to improve its capabilities, data prove to be the foundation of the building: "A solid data foundation is critical for executing a cloud-based enterprise data strategy that provides trusted information to decision makers." The transition to cloud computing is a profound transformation – organizational, institutional and technological.
Big Data	
DoD and Big Data[236]	The American army seems to place a great deal of hope

232 Chris Kubic, DoD Cloud Computing Security Challenges, December 2012, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-IA-challenges_ISPAB-Dec2008_C-Kubic.pdf.

233 Department of Defense, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, Washington, p. 4, 15 December 2014, http://iase.disa.mil/Documents/commercial_cloud_computing_services.pdf.

234 Henry Kenyon, DoD Changes Cloud Computing Policy, InformationWeek Government, 17 November 2014, http://www.informationweek.com/government/cloud-computing/dod-changes-cloud-computing-policy/d/d-id/1317511.

235 – Army Cloud Computing Strategy, Office of the Army Chief Information Officer, version 1.0, p. 40, 15 May 2015, http://ciog6.army.mil/Portals/1/Army_Cloud_Computing_Strategy%20Final_v1_0.pdf.

– Colonel Scott A. Smith, Future of Department of Defense Cloud Computing Amid Cultural Confusion, A.S. Army War College, 32 pages, 2013, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA589450.

	in the analytic capabilities of Big Data ("Big data is an ecosystem consisting of data collection, storage and computation architecture and analytics")[237] – technologies which help to preserve its informational dominance[238]: – scanning social networks in multiple languages, applying big–data processing to them, and searching for economic, social, political (etc.) information, almost in real time, using a simple smart-phone[239]; – predictive analysis must contribute to decision–making, to anticipating the enemy's maneuvers[240], to the management of specific problems (e.g. suicides in the forces).241 However, the aim is not to try to predict the outcome of conflicts or wars, but instead to find a way to better prepare the defensive forces against all eventualities[242]; – just like the use of cloud computing, big data is presented as a way to save money for the DoD[243].

Table 4.15. *Data in the United States' defense strategies*

236 Army Research Laboratory Technical Implementation Plan, 2015-2019, US Army RDECOM, p. 92, January 2015, http://www.arl.army.mil/www/pages/172/docs/ARL_Technical_Implementation_Plan.pdf.

237 Air Force Brig Gen Brian Dravis, chief of the Defense Information Systems Agency (DISA) Joint Information Environment Technical Synchronization Office, cited in "Big data takes a strategic turn at DoD", 21 November 2014: http://archive.c4isrnet.com/article/20141118/C4ISRNET14/311180008/Big-data-takes-strategic-turn-DoD.

238 Michael Hardy, Big Data plays key role in Army technical plan, C4ISR&Networks, 6 February 2015: http://www.c4isrnet.com/story/military-tech/it/2015/02/26/army-technical-implementation-plan/24060299/.

239 Kevin McCaney, Army intel wants to scan social media from 40 countries, Defense Systems, 17 December 2013: https://defensesystems.com/articles/2013/12/17/army-intell-social-media-big-data.aspx.

240 Army Research Laboratory Technical Implementation Plan, 2015-2019, US Army RDECOM, January 2015, 92 pages: http://www.arl.army.mil/www/pages/172/docs/ARL_Technical_Implementation_Plan.pdf

241 Patricia Kime, Soldiers' suicide risk predictable with Big Data, study says, Military Times, 12 November 2014: http://www.militarytimes.com/story/military/2014/11/12/big-data-suicide-risk/18907171/.

242 Putting Predictive Analytics to Work for the Army – An Executive Perspective, Government Executive, 30 April 2015: http://www.govexec.com/govexec-sponsored/2015/04/putting-predictive-analytics-work-army-executive-perspective/111406/.

243 Christopher Short, Big Data's $ 1.6B role in DoD's IT Strategy, Fedscoop, 7 July 2015 http://fedscoop.com/big-datas-1-6-billion-role-in-dods-it-strategy.

4.3.4.2. *Defining "data warfare"*

A data-centered approach would shift the boundaries of information warfare. A definition of data warfare could integrate:

– the struggle for data:

- collecting and preventing the adversary from collecting data,

- managing sensors and data streams; preventing the enemy from accessing the sensors and data streams (protection); interfering with enemy senses and data streams;

– the objectives of data mastery:

- intelligence,

- surveillance, monitoring,

- detection of weak signals upstream of the production of information,

- selection, sorting of data upstream of the production of information,

- fooling the enemy sensors,

- maintaining the advantage, in time and space, over the enemy in terms of the capacity for collection and processing of data;

– the challenges of data management:

- the placement of the sensors,

- the definition of the choice of sources with a view to the final use of the data,

- the quality of the source data,

- the quality of the sensors,

- the capacity for processing the collected data,

- the hardening of the data (or of the collection, processing and storage systems). Whilst the collection and transmission of data represent technical challenges, storage and protection of data streams are crucially important, but are still a long way from being perfect.

The expression "data warfare" was introduced in the 1990s, in an article by Lawrence G. Downs Jr[244].

	Author	Year
"Digital Data Warfare (DDW) is malicious computer code covertly introduced into one or more specific computer systems or networks, by an attacker to meet military, political, economic or personal objectives […] It is one of the many weapons an information warrior may use to ply his trade"[245].	Lawrence G. Downs Jr (USA)	1995
"Information warfare comprises two major branches – radiation warfare (RW) and *data warfare* (DW) […] Semantically, information warfare is more accurately DW, in that both good information and disinformation consist of data. Leaving aside the theoretical distinctions, DW essentially involves obtaining control over opponents' processing, analysis and decision–making infrastructure in order to make it act in your interests rather than theirs. DW can range from infecting computers via well–known techniques such as internet–borne viruses, to inserting disinformation into a radio data stream through highly classified techniques with specialised equipment"[246].	Richard B Gasparre	2009
Data warfare may denote a set of practices[247] intended to fool the algorithms.	Alistair Croll[248]	2013

Table 4.16. *Definitions of the expression "data warfare"*

244 Lawrence G. Downs Jr, Digital data warfare: using malicious computer code as a weapon, Air War College, United States, p. 38. http://www.dtic.mil/dtic/tr/fulltext/u2/a424872.pdf.

245 This definition and that of the objectives and methods of DDW correspond to CNOs (computer network operations – CAN and CND). This involves using cyber attacks to achieve particular objectives. Code is the weapon in these operations.

246 Richard B Gasparre, Redefining Warfare's Electromagnetic Spectrum, 25 March 2009, http://www.army-technology.com/features/feature51510/.

247 Injecting noise, googlebombing, mistraining the algorithms.

248 Alistair Croll, Stacks get hacked: The inevitable rise of data warfare, 18 January 2013, http://radar.oreilly.com/2013/01/data-warefare.html.

Conclusion

Humans are on a never-ending quest for power. Ideologies and religions, and the accumulation of capital and wealth, allow some people to submit and others to dominate, and offer sufficient reasons for conflict to attempt to impose one's will on other people. Technological innovation is often essential in this quest for power, because controlling technology, with the advantage it lends, depends on the ability to dominate the other party. Thus, telecommunications, computer technology, networks, the Internet and information have not only served humanistic, utopian, egalitarian objectives and technological progress, but also, of course, served the financial objectives of industries (economic power) as well as the interests of the defense forces (military power through technological advantage) and political forces (power of control and monitoring populations, for example). Each innovation has its promises of new powers: the holders of absolute power conferred by mastery of information technologies at the start of the 1990s may have believed in the possibility of winning Blitzkriegs; social media in the 2000s seem to have given people oppressed by authoritarian regimes the power to revolt, and citizens the ability to organize to fight for greater justice. Undeniably, these technologies have altered some of the ratios of strength, and have had a profound impact on the organization of the military forces and on the exercise of power, but they have not been able to achieve objectives which are perhaps aiming too high, such as those mentioned above.

Information Warfare, First Edition. Daniel Ventre.
© ISTE Ltd 2016. Published by ISTE Ltd and John Wiley & Sons, Inc.

All these evolutions only produce partial, time-limited forms of power. The technologies are replaced by others, and are then disseminated. Their effectiveness soon becomes reduced and spatially limited, as soon as resistance or obstacles are established (e.g. censure, prohibited or regulated markets, etc.), whether the adversaries/enemies have invested in the same technologies or have learned to prevent their effects. Thus, no technology can offer absolute power.

The form of power offered by technology is a subject of constant debate. Such was the case with information technologies. In the 1990s, the military investigated their nature, the place of NICT in the organization of the defense forces and in strategy (debates about the revolution in military affairs).

Although it is recognized that information plays a crucial role in the exercise of strength and power, this is not always sufficient. Action in the information space sometimes heralds the onset of more conventional military operations, but does not determine the outcome of the conflicts. The same debates have been raging for two decades on the subject of cyber operations, but paradoxically, it is easier to agree that cyberspace alone is not capable of achieving these political objectives, and winning conflicts (imposing one's will on the adversary/enemy). Cyber operations serve as a support, to complement conventional operations, in parallel.

It is our opinion that in this evolution from an information-centered train of thought to one centered on cyber, today there is a third period, centered on data. Even now, the data-centered approach cannot escape its cohort of utopian views and beliefs. Success in the conflict, and national security, involve – are reliant upon, even – the exploitation of data. Armies have begun to engage in cloud computing, have become aware of the vulnerability of their masses of data with the Snowden affair and the theft, in 2015, of the databases of US Defense personnel. The keyword today is "big data", which denotes combining heterogeneous masses of data with powerful processing tools (calculators and algorithms), in order to extract meaning from the data – sometimes even those data which, *a priori*, hold little interest. Police forces today, but also armies, are making full use of big data (and all that the technique promises: rendering data useful, making it talk,

discovering, seeing the invisible and – which is the ultimate goal – predicting data). The effects of these influences will be felt for several years to come, until a new logic is developed to substitute this one; until the emergence of a new technology, and new substitution paradigms.

Today, the struggle for data mastery is becoming organized. The data-centered approach takes the spotlight away from the ordinary citizen. Undeniably, he or she is a user and an Internaut, and his/her daily life is filled with data. Citizens are both producers and consumers of data, by way of the services offered to them by industry. Yet the main function fulfilled by ordinary citizens is to provide and produce data, enrich the databases about themselves, and enrich the data universe. It is no longer feasible for any and all such citizens to master the exploitation of the masses of data produced, to collect them, manipulate them, process them, extract added value from them and turn them into instruments of power. Indeed, in order to do so, excellent technical capabilities are needed; we need skills and technical knowledge. We must master algorithms. In the world of data, the individual is essentially a sensor, a source of data which can then be used by a merchant (to adapt the products and services they offer on the basis of their knowledge of the consumer/client, whether that be a simple individual, a business or a state), or by politicians and the State. The algorithm is one of the essential driving forces in this struggle for and with data. Human intervention remains absolutely crucial in the initial phase of implementation of the means of data collection/processing (deciding on which data to collect, the methods to be used, and their end goals). However, it may soon be relegated to the background, when the mass of data and the processing speed surpass human capabilities.

Index

B, C, D

blogs, 190, 198
C4ISR, 72, 131, 137, 141, 151, 212
command and control (C2C), 4, 17, 44, 60, 64–67, 97, 129, 141, 222, 224, 229, 235
cyber war, 23, 147, 193, 195, 197, 198, 207, 211, 213, 222, 226, 235
cyber warfare, 4, 5, 133
CyberSA, 77
cyberspace, 138, 147, 150, 159, 187, 189, 195, 198, 202, 203, 207, 209, 211–213, 233
CyNetOps, 77
deception, 9–12, 14–18, 21, 26, 28, 44–46, 66, 67, 113, 114, 127, 129, 150, 158, 224, 228, 229, 231
defacements, 188, 199, 202, 210, 211, 213
dominance, 6, 8, 15, 24, 52, 54, 55, 113, 129, 133, 150, 227

E, G, H, I

electronic warfare, 4, 5, 7, 9, 11, 12, 16, 17, 25, 26, 45, 46, 66, 112, 113, 129, 133, 137, 150, 193, 226, 228, 235
espionage, 2, 25, 46, 111, 127, 136, 139, 148, 149, 167, 168, 226, 235
Geneva convention, 60
Goldwater-Nichols Department of Defense Reorganization, 1986, 10
guerilla, 70, 130
hacker, 4, 5, 90, 108, 114, 130, 147
hacking, 132, 134, 135, 191, 196, 209, 212, 213, 233, 235
hacktivists, 90, 134, 135, 147, 198, 205, 209, 212
information
  operations, 7, 8, 10–14, 19, 23–27, 44, 45, 54, 66, 67, 74, 75, 112, 132, 151, 213, 223, 230, 231
  warfare, 1–9, 11, 13, 14, 23, 24, 26, 64, 67

Information Warfare, First Edition. Daniel Ventre.
© ISTE Ltd 2016. Published by ISTE Ltd and John Wiley & Sons, Inc.

L, M, N, O

law, 108, 126, 189, 202
misinformation, 3, 15, 127, 194, 205, 206, 209, 210, 230, 231
Network Centric Warefare (NCW), 72, 73, 90
netwar, 85, 86, 89, 90, 113, 129, 147, 244, 245, 271, 276
nuisance, 199
OODA, 26, 30, 58, 60, 67, 69, 73, 90, 224, 230, 234, 275

P, R, S

pirates, 186
propaganda, 12, 15, 25, 46, 47, 61, 129, 158, 190, 195, 202, 209, 226, 228, 230, 231
psychological
operations, 3–5, 9, 11, 16, 25, 26, 46, 47, 114
warfare, 113, 114, 129, 141, 158
Revolution in Military Affairs (RMA), 70, 94, 115, 116, 137, 143
rumors, 27, 64, 110, 191
shashoujian, 139–141, 145
strategy, 7, 13, 62, 106, 111, 112, 114, 115, 125, 127, 130, 138, 139, 141–145, 147, 149, 150, 152, 156, 187, 204, 227, 232
superiority, 8, 10, 24, 52, 53, 69, 96, 97, 105, 111, 114, 133, 140, 146, 194, 204, 224, 233, 234

T, U, V, W

target, 3, 4, 19, 21, 27, 28, 30, 46, 49, 52, 56, 60, 61, 72, 82, 83, 104, 112, 125, 131, 134, 135, 146, 147, 149, 170, 172, 202, 213, 217, 223, 226, 230–232
terrorism, 46, 71, 83, 94, 95, 106, 111, 116, 120, 154, 187, 226, 246, 266, 271, 281, 308
threat, 14, 60, 112, 114, 116, 136, 141, 146, 148, 153, 154, 156–159, 199, 204, 208, 223, 232, 233, 235
United Nations, 156, 157
victim, 134, 136, 171–173, 190–192, 201, 207, 217, 224, 244, 284, 294, 303
virus, 3, 4, 23, 110, 208, 216, 218
weapon, 2, 4, 7, 14, 17, 56, 60–62, 65, 104, 110, 111, 116, 130, 131, 140, 148, 156, 189, 194, 235

Other titles from



in

Information Systems, Web and Pervasive Computing

2015

ARDUIN Pierre-Emmanuel, GRUNDSTEIN Michel, ROSENTHAL-SABROUX Camille
Information and Knowledge System
(Advances in Information Systems Set – Volume 2)

BÉRANGER Jérôme
Medical Information Systems Ethics

BRONNER Gérald
Belief and Misbelief Asymmetry on the Internet

IAFRATE Fernando
From Big Data to Smart Data
(Advances in Information Systems Set – Volume 1)

KITAJIMA Munéo
Memory and Action Selection in Human–Machine Interaction
(Human-Machine Interaction Set – Volume 1)

KRICHEN Saoussen, BEN JOUIDA Sihem
Supply Chain Management and its Applications in Computer Science

NEGRE Elsa
Information and Recommender Systems
(Advances in Information Systems Set – Volume 4)

POMEROL Jean-Charles, EPELBOIN Yves, THOURY Claire
MOOCs

SALLES Maryse
Decision-Making and the Information System (Advances in Information Systems Set – Volume 3)

SAMARA Tarek
ERP and Information Systems: Integration or Disintegration
(Advances in Information Systems Set – Volume 5)

2014

DINET Jérôme
Information Retrieval in Digital Environments

HÉNO Raphaële, CHANDELIER Laure
3D Modeling of Buildings: Outstanding Sites

KEMBELLEC Gérald, CHARTRON Ghislaine, SALEH Imad
Recommender Systems

MATHIAN Hélène, SANDERS Lena
Spatio-temporal Approaches: Geographic Objects and Change Process

PLANTIN Jean-Christophe
Participatory Mapping

VENTRE Daniel
Chinese Cybersecurity and Defense

2013

BERNIK Igor
Cybercrime and Cyberwarfare

CAPET Philippe, DELAVALLADE Thomas
Information Evaluation

LEBRATY Jean-Fabrice, LOBRE-LEBRATY Katia
Crowdsourcing: One Step Beyond

SALLABERRY Christian
Geographical Information Retrieval in Textual Corpora

2012

BUCHER Bénédicte, LE BER Florence
Innovative Software Development in GIS

GAUSSIER Eric, YVON François
Textual Information Access

STOCKINGER Peter
Audiovisual Archives: Digital Text and Discourse Analysis

VENTRE Daniel
Cyber Conflict

2011

BANOS Arnaud, THÉVENIN Thomas
Geographical Information and Urban Transport Systems

DAUPHINÉ André
Fractal Geography

LEMBERGER Pirmin, MOREL Mederic
Managing Complexity of Information Systems

STOCKINGER Peter
Introduction to Audiovisual Archives

STOCKINGER Peter
Digital Audiovisual Archives

VENTRE Daniel
Cyberwar and Information Warfare

2010

BONNET Pierre
Enterprise Data Governance

BRUNET Roger
Sustainable Geography

CARREGA Pierre
Geographical Information and Climatology

CAUVIN Colette, ESCOBAR Francisco, SERRADJ Aziz
Thematic Cartography – 3-volume series
Thematic Cartography and Transformations – volume 1
Cartography and the Impact of the Quantitative Revolution – volume 2
New Approaches in Thematic Cartography – volume 3

LANGLOIS Patrice
Simulation of Complex Systems in GIS

MATHIS Philippe
Graphs and Networks – 2nd edition

THERIAULT Marius, DES ROSIERS François
Modeling Urban Dynamics

2009

BONNET Pierre, DETAVERNIER Jean-Michel, VAUQUIER Dominique
Sustainable IT Architecture: the Progressive Way of Overhauling Information Systems with SOA

PAPY Fabrice
Information Science

RIVARD François, ABOU HARB Georges, MERET Philippe
The Transverse Information System

ROCHE Stéphane, CARON Claude
Organizational Facets of GIS

VENTRE Daniel
Information Warfare

2008

BRUGNOT Gérard
Spatial Management of Risks

FINKE Gerd
Operations Research and Networks

GUERMOND Yves
Modeling Process in Geography

KANEVSKI Michael
Advanced Mapping of Environmental Data

MANOUVRIER Bernard, LAURENT Ménard
Application Integration: EAI, B2B, BPM and SOA

PAPY Fabrice
Digital Libraries

2007

DOBESCH Hartwig, DUMOLARD Pierre, DYRAS Izabela
Spatial Interpolation for Climate Data

SANDERS Lena
Models in Spatial Analysis

2006

CLIQUET Gérard
Geomarketing

CORNIOU Jean-Pierre
Looking Back and Going Forward in IT

DEVILLERS Rodolphe, JEANSOULIN Robert
Fundamentals of Spatial Data Quality

Information warfare has been an issue at the heart of the debate about the revolution in military matters since the 1980s. Although this concept appears to be used less than it once was, it is by no means obsolete.

This book introduces the concept of "information warfare", covering its evolution over the last decade. In this second edition, the author chooses to focus on three states: the USA, China and Russia, and offers a detailed analysis of the evolution of the theories, concepts and doctrines employed in those countries.

As a modest contribution to the strategic study of modern conflict, the book asks the following questions: do the terms "information warfare", "information operations" and "cyberoperations" all denote the same reality? Do states perceive and talk about the same threats today as they did 20 years ago? Do the actors, principles and logics of information warfare still remain the same?

Daniel Ventre is an engineer at the CNRS (CESDIP laboratory) and holder of the Chair in Cybersecurity and Cyberdefense at Ecoles de Saint-Cyr Coëtquidan, as well as a lecturer at Telecom ParisTech in France.

ISTE
www.iste.co.uk
WILEY
9 781848 216600