INFORMATION SYSTEMS, WEB AND PERVASIVE COMPUTING SERIES

Information Warfare

2nd Edition revised and Updated

Daniel Ventre

iSTE WILEY

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.

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

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

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.

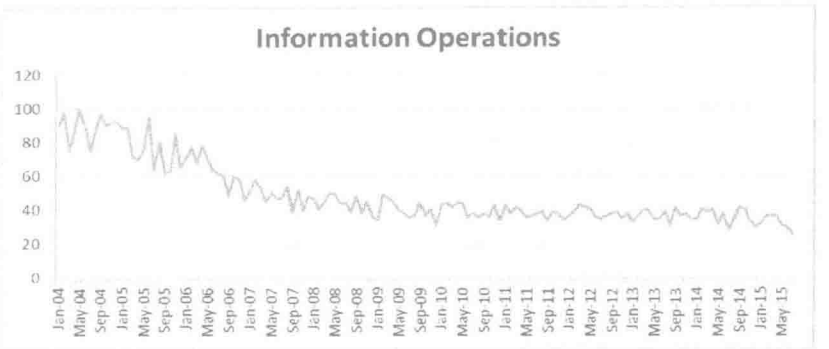

Figure I.2. *Google Trends. Evolution in number of searches for the term "Information Operations"*[2]

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?

Contents

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

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/.