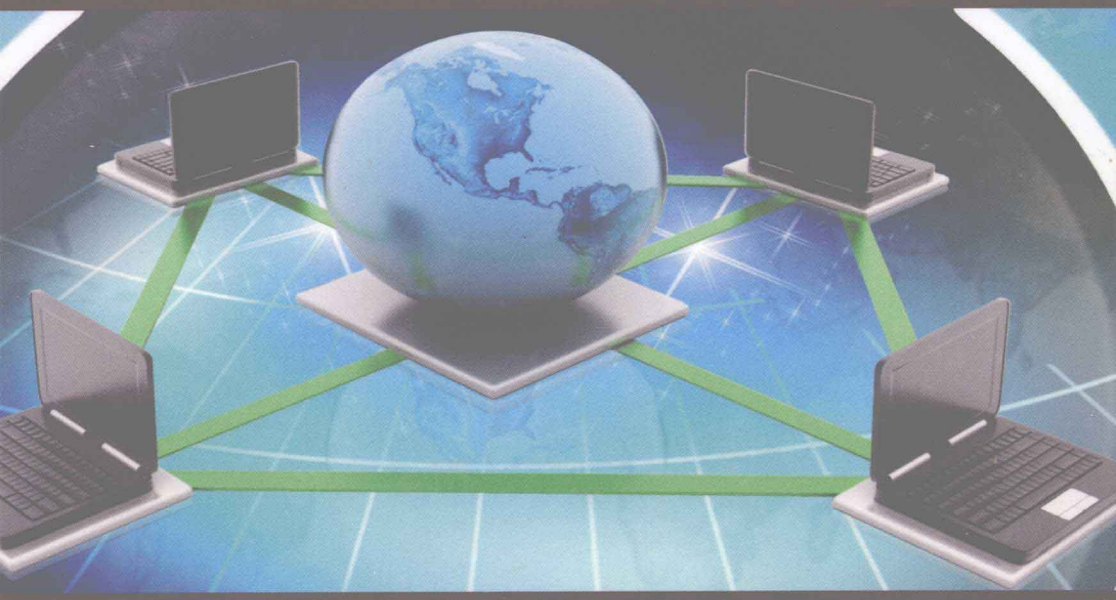

Cyberwar and Information Warfare

Edited by
Daniel Ventre

ISTE
WILEY

Cyberwar and Information Warfare

Edited by
Daniel Ventre

ISTE
WILEY

First published 2011 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 Cataloging-in-Publication Data

Cyberwar and information warfare / edited by Daniel Ventre.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-84821-304-3
1. Information warfare. 2. Psychological warfare. 3. Computer crimes. I. Ventre, Daniel.
U163.C937 2011
355.3'43--dc23

2011024020

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-304-3

Printed and bound in Great Britain by CPI Antony Rowe, Chippenham and Eastbourne.

Cyberwar and Information Warfare

Introduction

Through a range of articles which suggest different and additional approaches, and following in the footsteps of the French experts in this domain, this book takes us into the concepts of information warfare and cyberwar.

Information warfare above all expresses the concept of conflict and the position of information in this context, and it brings conflict into the perspectives of technology and the information society. It is both a war in cyberspace, and a war of ideas. In *Ecran/Ennemi*, François-Bernard Huyghe[1] defines information warfare as "any activity intended to get data and knowledge (and to deprive the enemy from it) for strategic means, either by systems (vectors and means of processing the information), or by content, by ensuring informational domination. Under its offensive perspective, it refers to any operation resorting to rumor, propaganda, computer viruses which corrupt or hijack an opponent's information or data flow, whether this is a State, an army, or a political or economic entity"[2]. It may also be understood as the aggressive/defensive use of components of informational space (information and information systems) in order to hit/protect the sovereignty of a State, by action taken in times of peace, crisis, or conflict [VEN 09].

Cyberwar, a technical dimension of information warfare, may be defined as the recourse to cybernetic capabilities to lead aggressive operations in cyberspace, against military targets, against a State or its society. It will also be defined as "a classic war, where at least one of the components, in execution, its motivations and tools (weapons in the broadest sense) is based on the computerized or digital field"[3].

Introduction written by Daniel VENTRE.

1 François-Bernard Huyghe, see Chapter 1.

2 [HUY 02].

3 Eric Filiol, see Chapter 4.

It is certainly a matter of "war" here, even if we understand that the term may raise problems due its metaphorical use for forms of confrontation which do not use lethal weapons, and do not result in "declarations of war" or "peace treaties". But, moreover, this may be due to the difficulty of making the distinction between a military operation, an act of war, a criminal act, and between a politically, ideologically, criminal or playfully motivated action. Even when it has a negative effect on the balance in our society (and even marginally if the State uses its methods and activists punctually), cybercriminality will not be included in our research here, and will be removed from the field of information warfare and cyberwar definitively. We will focus on more threatening forms of action taken in informational space, which are either destabilizing or destructive, and which target the most vulnerable, important components of our society: our sovereignty, our culture.

At the time when the important, but also the most modest, nations of this world seem confronted with the whole range of cyberattacks, the questions asked by those working for security and defense concern aggressive as much as defensive potentials offered by their own information systems, and of course, those of their competitors or opponents, or even their partners.

The French White Paper on Defense and National Security [GOU 08], and the report by Senator Roger Romani on cyberdefense [ROM 08] have clearly placed the issue of information system security on the same rank as defence and national security.

In 2005, the Labordes report [LAS 05] adopted the same perspective, by considering information system security (ISS) as "an issue on a national scale [...] For the State, national sovereignty is at stake. In fact, it is responsible for ensuring the security of its own information systems, the operational continuity of vital institutions and infrastructures for the country's socio-economic activity and protecting companies and citizens".

Armed with this knowledge and political will, the country is therefore not so sheltered from risks, especially when they are difficult to apprehend, and when their production is unpredictable.

In this way, and in the same way as all industrialized countries which are developing a relatively high level of independence in relation to cyberspace, in recent years France has been caught up in the ever growing waves of what we call cyberattacks (attacks against the French Atomic and Alternative Energies Commission in 2006: French diplomats suffering hacked emails, Rafale fighter planes "nailed to the ground", victims of the Conficker impact, etc.).

According to the Romani report, these incidents would have "materialized a still badly identified threat to our continent in a very concrete way, particularly in France". The report proposes a brief list of possible reasons for these flaws in security which are common to all modern States: system interconnections, their relation to the Internet, the contaminating nature of the Internet (everything which comes into contact with it becomes fallible), society's dependence on information systems, the permeability of informational space due to portable equipment (threat to network integrity), flaws in Internet protocol, use of applications (off-the-shelf software) which add to the complexity and flaws in security, contamination of the most solid software by the weakest, etc.

If the positive aspects of the technological revolution of information build the structure of our modern society, then threats of deconstruction are just as high. At the turn of the 1990s, the USA expressed its approaches to information warfare, revealing their ambitions for exploiting and dominating informational space, followed by other large nations. Today, all those intent on getting themselves a place in the mix of nations are considering the possibilities offered by cyberspace as a platform for confrontation and expressing their power. But alongside these groups, we also find those who pay little regard to the doctrines of those in power, and who endeavor to be on a par with them, turning around their traditional forces and challenging them in informational space. This is the combined action of legitimate and illegitimate forces, bred by the instability and insecurity in cyberspace. This is without even mentioning actions of ordinary cybercriminality. All these parties exploit technical flaws, the weaknesses in architecture and its components, and use these weaknesses as their means of force and capacities.

Of course, vulnerability to risk is not exclusive to French systems. With several billions of dollars, the USA is (in pursuit of their quest to dominate cyberspace) also under strain to secure their technological scaffolding, under stresses of alarming discussions on security: "If the nation went to war today in a cyberwar, we would lose. We are the most vulnerable. We are the most connected. We have the most to lose", spoke out Michael McConnell, executive vice-president of American National Security business Booz Allen Hamilton, in February 2010[4].

This type of catastrophic address is, of course, often dictated by direct mercenary interests. But it is also part of an older line of thinking, which sees certain sources of weakness, and societal or civilizational vulnerability in technological power.

This is an interesting question. Has the technological information revolution, which shaped our civilization during the second half of the 20th Century, really changed our vision of the world?

---

4 www.zdnetasia.com/news/security/0,39044215,62061413,00.htm?scid=nl_z_ntnd.

The new world. This is the world in the aftermath of the Cold War, scarred by the attacks of 9/11. It is globalization which creates a world "[...] neither better nor more dangerous" yet "clearly more unstable" (the proof is in the financial crisis of Fall 2008). It is a world which remains dominated by the USA's power but which has a rebalancing effect, to the advantage of Asia, and with:

– new threats (terrorism, ballistic missiles, attacks on information systems, espionage, organized crime networks);

– the gradual disappearance of the distinction between internal and external security;

– a necessary global approach to problems;

– more complexity and uncertainty which make our environment and its threats difficult to apprehend;

– an increase in military spending throughout the world;

– a fragile system of collective security.

This new world also confirms cyberspace as a vital system, a nervous system, of our model of society. Information is more widely spread and much more quickly in cyberspace, with a resultant sped-up action, more media power (The White Paper refers to the "CNN effect"), an uncontrolled flow of ideas, particularly those concerning ideological, religious, and radical contestations, a power gained for non-State groups and a reduced expression of the capacity to control, and State sovereignty. "The staggering acceleration of the circulation of information...makes the States' capacity for autonomous intervention fragile", is written in the White Paper from 2008. This is also a new world which creates a new space out of nothing (cyberspace) and which puts all its hopes into it (economy, a more open, fairer, more equal society). But it also transforms its power and therefore its violence, its crises, its conflicts, as it is a matter of finding the limitations of its sovereignty within it, and defending them.

For all this, if technologies are new, if the global context evolves, we cannot help but notice that constant factors exists in the way mankind may represent technological power and the associated fears (risk, threat, violence, war).

> "Wireless telegraphy and telephony were being used right across Europe, and were so easy to use that even the poorest of men could speak to a man located at any point on the globe, how he wanted, when he wanted [...] This was the abolition of borders. A critical time for all! [...] The French Republic, The German Republic [...], the Swiss Republic and Belgium (sic), all expressed by unanimous vote in parliament and in several meetings, the solemn resolution to defend

> national territory and industry against any foreign aggression. Forceful laws were promulgated [...], ruling out the use of wireless telegraphy [...]. Our borders are defended by electricity. A fire zone reigns supreme around the federation. A small, bespectacled man sitting somewhere, anywhere, in front of a keyboard. This is our only soldier. He just has to lay his finger on one button to pulverize an army of 500,000 men".

This article seems extremely modern. However, it is signed by Anatole France and dates back to 1905. In this writing, entitled *Sur la Pierre Blanche* (On the White Stone) [FRA 05], we may recognize very contemporary themes from the start of our 21st Century. They include threats to national defence and security, the negative equivalent (in the eyes of leaders) of the new freedom of communication offered to the people, the threat of foreign attack born out of using these communication technologies, authoritarian and lawful reactions when aware of this threat, and the cooperation of European powers when faced with informational threats. Moreover, we recognize the theme of absolute power which can be found concentrated in the hands of a single man (the hacker sitting in front of his keyboard who became the soldier), as powerful on his own as a whole army (concept of asymmetry). In one single move he is capable of destroying an opponent (the utopia of all technological powers, the will to defeat without confrontation, the war of networks). This is an apocalyptic discourse, reminding us of the catastrophic predictions of an electronic Pearl Harbor (discourse on major threats, collapse of a model society, fatal strategic surprise).

The article writers' relationship with electronic space greatly resembles the relationship that our peers have with cyberspace. Is this wrong, or right?

Faced with this knowledge, and aiming to pull itself away from sometimes exaggerated representations of the role and capacities of informational space and information technologies (apocalyptic and utopic discourse), this collective work by a few French experts having put a vast amount of effort into the themes of information warfare, cyberwar, information and communication, and security and defence, wish to propose a tool for understanding the mechanisms, logic, and modalities which characterize the power struggles within informational space. This is (space of ideas and cyberspace) one of these places where State power and influence will manifest itself. It is a space to be conquered. But States are being challenged by real heavy threats in these spaces with evasive borders. Therefore, in order to respond to the expectations written into the White Paper, as far as the security of our information systems and our sovereignty are concerned, we must measure up the stakes, the capacities and the modes of action which could be used by an aggressor, so that they may defend themselves better, by themselves.

The authors of this collection propose a reflection on key concepts which are: information (in terms of data, messages, knowledge, programs), war, attack, strategic surprise, (military) information warfare, cyberwar, the nature of "cyberwars" or "information warfare", the position of cyberwars in warfare, of cyberspace in conflict, dimensions (of conflict, of cyberspace and information warfare), borders, the enemy (difficulty of identifying, locating, and defining it), power struggles between cybernetic conflict activists, interaction between knowledge and violence, between the real world and cyberspace, the transfer of conflict into cyberspace, the role of politicians when confronted with cyberwars, the victim's political attitude, the strategy (offensive and defensive), the consequences of applying the term "war" to cybernetic attacks, the relationship between the West and non-Western world, the relationship that Western democracies could or must have with the war of meaning and cyberwar in order to retain their vision of the world and their power.

On the other hand, this book proposes an insight into the technical, operational, and strategic dimensions of a cyberattack. This includes the accompanying role played by cyberwar (in relation to classic military operations), the importance of combining old strategies with technology, the imputability of attacks, the limits imposed by the impossibility of a backlash (where the aggressor cannot be identified), the difficulty of defining and understanding the rules to be applied in the absence of direct combat, the essential characteristics of cyberwar; obliterating space (ignoring distances and borders), time (surprise), proof (the attacker operates with complete impunity), the attacker's advantage gained on the target, the aggressor's power, the position of human beings in cyberattacks and in cyberspace.

Individuals are the major cogs in important infrastructures, and they make up the easy and favored targets that we can hit via cyberspace (rumors, misinformation, and personal data exploitation). This book will also include the manipulation of reality, the major importance of strategic and tactical frameworks and methods which are capable of giving an aim to cyberwar, and to cyberattacks which are capable of putting together operations in the pursuit of well defined aims. It also includes the vital role of information, the exploitation of paralysis brought on by a strategic surprise cyberattack, the choice of targets, the extent of the attack's impacts when carried out electronically, the real effects on organizations which have been attacked, identification of the manifestations of reciprocal interactions between humans and systems, between the "real" and the "virtual".

The first four chapters compose the theoretical and conceptual part of the book:

– *Cyberwar and its Borders* (François-Bernard Huyghe) which is an interrogative and mediological chapter;

– *War of Meaning, Cyberwar and Democracies* (François Chauvancy), dealing with the historical-cultural factors of a new polemology;

– *Intelligence, the first Defence? Information Warfare and Strategic Surprise* (Joseph Henrotin), a strategy analysis;

– *Cyberconflict: Stakes Of Power* (Daniel Ventre), on the geopolitical dimension of cyberconflict.

The last three chapters offer a more practical, empirical, and operational approach:

– *Operational Aspects of a Cyberattack, Information, Planning and Conduct* (Eric Filiol), thus analyzes the connection between the attack and general strategies;

– *Riots in Xinjiang and Chinese Information Warfare* (Daniel Ventre) analyzes the Chinese strategy when confronted with an internal crisis;

– *Special Territories* (Daniel Ventre) deals with information warfare and cyberwar in North Korea and Hong Kong.

Bibliography

[FRA 05] FRANCE A., *Sur la Pierre blanche*, fr.wikisource.org/wiki/Sur_la_pierre_blanche, Paris, France, 1905.

[HUY 01] HUYGHE F.B., *L'ennemi à l'ère numérique*, PUF, Paris, France, 2001.

[HUY 02] HUYGHE F.B., *Ecran/Ennemi. Terrorismes et guerres de l'information*, www.huyghe.fr/dyndoc_actu/424eb3aed503a.pdf, Editions 00h00, Paris, France, 2002.

[LAS 05] LASBORDES P., *La sécurité des systèmes d'information, un enjeu majeur pour la France,* www.mag-securs.com/IMG/pdf/rapport_Pierre_Lasbordes.pdf, Paris, 26 November 2005.

[GOU 08] GOUVERNEMENT FRANÇAIS, Le livre blanc sur la défense et la sécurité nationale, Odile Jacob, Paris, France, 2008.

[ROM 08] ROMANI R., Rapport d'information fait au nom de la Commission des Affaires étrangères, de la défense et des forces armées sur la cyberdéfense, Sénat, www.senat.fr/rap/r07-449/r07-4491.pdf, Paris, France, 8 July 2008.

[VEN 09] VENTRE D., *Information Warfare*, ISTE Ltd, London and John Wiley & Sons, New York, 2009.

List of Acronyms

AFCYBER	Air Force Cyber Command
ANSSI	*Agence nationale de la sécurité des systèmes d'information* (National Security Agency Information Systems)
APCERT	Asia Pacific Computer Emergency Response Team
ARCYBER	Army Cyber Command
ASAT	Anti-Satellite Technologies
ASIO	Australian Security Intelligence Organisation
AusCERT	Australia Computer Emergency Response Team
BCS	Baltic Cyber Shield
BPC	Bipartisan Policy Center
C2	Command & Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAHK	Communication Association of Hong Kong
CARIS	Chemical Accident Response Information System
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CC-IN2P3	*Centre de calcul de l'IN2P3* (A computing center in Villeurbanne, France)
CDX	Cyber Defense Exercise
CEPA	Closer Economic Partnership Agreement

CERN	European Laboratory for Particle Physics
CERT	Computer Emergency Readiness Team
CIA	Central Intelligence Agency
CID	Confrontations in the Information Dimension
CNN	Cable News Network
CND	Campaign for Nuclear Disarmament
CNO	Chief of Naval Operations
CNRS	*Centre National de la Recherche Scientifique* (National Center for Scientific Research)
CSOC	Cyber Security Operations Centre
CSS	Central Security Service
CyberOps	Cyber Operations
CyberSA	Cyber Situational Awareness
CyberSpt	Cyber Support
CyNetOps	Cyber Network Operations
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DPRK	Democratic People's Republic of Korea
ENISA	European Network and Information Security Agency
FEMA	Federal Emergency Management Agency
GCHQ	Government Communication Headquarters
HKCERT	Hong Kong CERT
HUMINT	HUMan INTelligence
IC3	Internet Crime Complaint Center
ICT	Information and Communication Technologies
IP	Internet Protocol
KAIST	Korea Advanced Institute of Science and Technology

LID	*Lutte Informatique Défensive* (Defensive Computing)
LIO	*Lutte Informatique Offensive* (Offensive Computing)
MyCERT	Malaysian Computer Emergency Response Team
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Center
NIS	National Intelligence Service
NSA	National Security Agency
ONI	Office of Naval Intelligence
OODA	Observe, Orient, Decide, Act
OOTW	Operation Other Than War
RFID	Radio Frequency Identification
RMA	Revolution in Military Affairs
SCADA	Supervisory Control and Data Acquisition
SGDSN	*Secrétariat général de la défense et de la sécurité nationale* (Secretary General for National Defence and Security)
SIGINT	SIGnal INTelligence
SingCERT	Singapore Computer Emergency Response Team
SNDC	Swedish National Defense College
UN	United Nations

Table of Contents