Information Warfare

Daniel Ventre

ISTE

WILEY

Information Warfare

Information Warfare

Daniel Ventre

iSTE

WILEY

First published 2007 in France by Hermes Science/Lavoisier entitled: *La guerre de l'information*
© LAVOISIER 2007
First published 2009 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

Ventre, Daniel.
[Guerre de l'information. English]
Information warfare / Daniel Ventre.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-84821-094-3
1. Business intelligence. 2. Trade secrets. 3. Information technology--Security measures. 4. Computer security--Management. 5. Data protection. I. Title.
HD38.7.V4713 2009
355.3'43--dc22

2009026202

British Library Cataloguing-in-Publication Data
A CIP record for this book is available from the British Library
ISBN 978-1-84821-094-3

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

FSC
Mixed Sources
Product group from well-managed forests and other controlled sources
Cert no. SGS-COC-2953
www.fsc.org
© 1996 Forest Stewardship Council

Table of Contents

Abbreviations

ACINT	Acoustic Intelligence
AFDD	Air Force Doctrine Document
AFIWC	Air Force Information Warfare Center
AFPD	Air Force Policy Directive
AIIT	Army Institute of Information Technology
APCERT	Asia Pacific Computer Emergency Response Team
ASCON	Army Static Switched Communication Network
BARC	Bhabha Atomic Research Center
BFT	Blue Force Tracking
BOA	Bulle Opérationnelle Aéroterrestre (“Air and Land Operations Bubble”)
C2	Command and Control
C2W	Command and Control Warfare
C3I	Command, Control, Communication, Intelligence
C4	Command, Control, Communication, Computers
C4I	Command, Control, Communication, Computers, Intelligence
C4I2SR	Command, Control, Communication, Computers, Intelligence, Information, Surveillance and Reconnaissance
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CBINT	Chemical and Biological Intelligence
CERT	Computer Emergency Response Team
CERT-In	Computer Emergency Response Team - India

CIA	Central Intelligence Agency
CMO	Civil-Military Operations
CNA	Computer Network Attacks
CNCERT/cc	China Computer Emergency Response Team/Coordination Center
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COMINT	Communications Intelligence
COMSEC	Communication Security
DDoS	Distributed Denial of Service
DIA	Defense Intelligence Agency
DISA	Defense Information System Agency
DIWA	Defense Information Warfare Agency
DoD	Department of Defense
DoDAF	Department of Defense Architectural Framework
DoS	Denial of Service
DPP	Democratic Progressive Party
DPRI	Defense Policy Review Initiative
DSO	Defense Science Organisation
DSTA	Defense Science and Technology Agency
EA	Electronic Attack
EBO	Effect-Based Operations
EDB	Economic Development Board
EIW	Economic Information Warfare
ELINT	Electronic Intelligence
EMP	Electromagnetic Pulse
EP	Electronic Protection
ES	Electronic Support
EW	Electronic Warfare
FAGCI	Federal Agency of Government Communications and Information
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FIWC	Fleet Information Warfare Center
FSB	Federal Security Bureau

GDP	Gross Domestic Product
HKCERT/cc	Hong Kong Computer Emergency Response Team/Coordination Center
HUMINT	Human Intelligence
IAD	Information Assurance Department
IBW	Intelligence Based Warfare
ICE	Integrated Control Enablers
ICT	Information and Communication Technologies
IDA	Infocomm Development Authority (of Singapore)
IED	Improvised Explosive Device
IFF	Identification Friend or Foe
IIT	Indian Institutes of Technologies
IKC2	Integrated Knowledge-based Command and Control
ILS	Integrated Logistics Support
IMINT	Image Intelligence
INDU	Indian National Defense University
INFOSEC	Information Security
IO	Information Operations
IP	Intellectual Property
IPv6	Internet Protocol version 6
ISC	Indian Science Congress
ISP	Internet Service Provider
ISR	Intelligence, Surveillance, Reconnaissance
IW-D	Information Warfare – Defense
IWSC	Information Warfare Support Center
JCS	Joint Chiefs of Staff
JDA	Japan Defense Agency
JEWEL	Joint modelling and simulation Environment for Wargaming and Experimentation Labs (Singapore)
JPCERT/cc	Japan Computer Emergency Response Team/Coordination Center
KGB	Komitet Gossoudarstvennoï Bezopasnosti
KISA	Korean Information Security Agency
KMT	Kuomintang
KrCERT/cc	Korea Computer Emergency Response Team
LIC	Low Intensity Conflict

LIWA	Land Information Warfare Activity
LTTE	Liberation Tigers of Tamil Eelam
MASINT	Measurement and Signature Intelligence
MDA	Media Development Authority
MILDEC	Military Deception
TARM	Tupak Amaru Revolutionary Movement
MyCERT	Malaysia Computer Emergency Response Team
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCW	Network Centric Warfare
NGA	National Geospatial-Intelligence Agency
NICT	New Information and Communication Technologies
NISS	National Institue of Strategic Studies
NIWA	Naval Information Warfare Activity
NSA	National Security Agency
NSCC	National Security Coordination Centre
NUCINT	Nuclear Intelligence
NUS	National University of Singapore
NGO	Non-Governmental Organization
OODA	Observation, Orientation, Decision, Action
OPSEC	Operations Security
ORNS	Operational Ready National Servicemen
OSINT	Open Source Intelligence
P2P	Peer to Peer
PAIR	Physical Action - Information - Response
PBA	Predictive Battlespace Awareness
PC	Personal Computer
PKK	Partiya Karkerên Kurdistan (Kurdistan Workers' Party)
PLA	(Chinese) People's Liberation Army
PSYOPS	Psychological Operations
PSYWAR	Psychological Warfare
RADINT	Radar Intelligence
RAHS	Risk Assessment and Horizon Scanning
RAW	Research and Analysis Wing

RINT	Radiation Intelligence
RMA	Revolution in Military Affairs
ROI	Return on Investment
SAF	Singapore Armed Forces
SBA/MBA	Singapore Broadcasting Authority/Media Development Authority
SCADA	Supervisory Control and Data Systems
SCME	Singapore Air Force Center for Military Experimentation
SIGINT	Signal Intelligence
SingCERT	Singapore Computer Emergency Response Team
SM3	Standard Missile-3
SMA	Singapore Manufacturer's Federation
SPIIRAS	St Petersburg Institute for Informatics and Automation of the Russian Academy of Science
SPRING	Standard, Productivity and Innovation Board
SVR	Sluzhba Vneshney Razvedki (Foreign Intelligence Service)
TECHINT	Technical Intelligence
TLD	Top Level Domain
TSU	Taiwan Solidarity Union
TWCERT/cc	Taiwan Computer Emergency Response Team/Coordination Center
WMD	Weapons of Mass Destruction

Introduction

While industry and society started imagining, creating and dreaming of new lifestyles for humanity with the evolution of information technologies, strategists were imagining new conflict scenarios for the 21st Century; how could we take advantage of information and information technologies to take the lead over our competitors or enemies?

The Gulf War in 1991 seemed to provide an early conclusive answer. Controlling information and its technologies is the key to victory against modern conflicts. The expression "information warfare" was recognized throughout the world as a new and major concept, becoming the object of concern for many decision makers and strategists, whether they were military or civilian.

During the 1990s, other concepts took root in these debates on the control, risks and challenges of information and new technologies, such as, for example, information operations, cyber warfare, computer network attack, network-centric war or cyber terrorism. Since then, international literature has abounded with books, articles, reports, studies, analyses and official, unofficial, serious, and even sometimes far-fetched expert comments, describing these concepts and theories ad infinitum. Today, in the military field, we sometimes prefer the expression "information operation", though we increasingly mention cyber warfare, infowar or cyber attacks; however, the basic concept remains the broader "information warfare", which includes a range of operations carried out within the information world.

Information technologies, presented as the primary vector of international growth in the 21st Century, seem also to be our worst enemy, the Achilles heel of our societies dependent on information systems because, through them and with them, our adversaries and enemies can attack us.

And attacks are widespread in cyberspace. They may vary in type (spamming, phishing, intercepting, intrusions, data leaks, site defacements and DoS[1] attacks) but they are all an attack. As for the attackers, they have long had the image of a hacker, sometimes a minor, wrongly portrayed as a prodigy of computer genius (as if one needed genius to type on a computer to attack systems), able to penetrate the computer systems of a bank or government agency alone, and even suspected of being able to launch a major and destructive attack against the networks of a nation. But attackers are not all teenagers desperate for a new game. There can be multiple profiles and motivations; attacks do not only take the form of hacker attacks.

More generally, the concern that cyber attacks can disrupt the economy of a corporation or a nation, or even affect global stability, has become the nightmare of countries dependent on information technologies. The world has become conscious that it has entered the information technology insecurity age, controlled by security vendors.

And, since it is no longer possible to do without information and information technologies, we might as well, while we're at it, do well by them and, if possible, be harmful to our enemies. How can we use information and information systems to increase our defence capabilities? How can we dominate the enemy? How can we defeat them?

Information warfare must respond to these expectations. It must provide nations that do not have the resources to reach the level of more powerful nations on a military, technological, economic and digital basis, the means to rival them. But for all that, information warfare is not the weapon of the poor, the rock that must be thrown at the giant's eye to blind him, because information warfare supposes that we have relatively significant technological means, financial means and, especially, strategies.

The expression "information warfare" has not found a single, consensual definition. The reason is undoubtedly in the terms that it is made up of. The term "warfare" is still the subject of many a debate and its definition is different whether we are a sociologist, anthropologist, economist, historian, political scientist or member of the military. As for "information", it is approached in a different way whether we are a mathematician, computer specialist, sociologist, journalist, member of the military or economist.

This book, which introduces the concept of "information warfare", is not meant to completely solve these questions of definition. Its objective is to analyze what information warfare can be, its multiple aspects and components (because

[1] Denial of Service.

information warfare cannot be reduced only to attacks against computer networks), to identify its players, challenges and possible strategies, as well as looking at the input of some of the larger nations, where the world's economic, political and military balances are decided at the beginning of the 21st Century.

Chapter 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 20 years.

1.1. Information warfare in the 1990s

1.1.1. *Points of view from security experts*

In 1994, in his book *Information Warfare* [SCH 94], 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. The United States is the target of economic and industrial espionage from Russia, from ex-members of the Eastern bloc, from Japan (which has almost destroyed the American information technology industry in Silicon Valley), and France and Germany who would not hesitate to use hackers to steal information;

– 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 that are 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) 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.

[1] [SCH 94], and for more recent approaches [SCH 02] and [SCH 05].

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].

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;

[2] Source: [THR 96].
[3] See [CAM 92] and [CAM 96].
[4] This concept is addressed in more detail later in this chapter.
[5] Read [DUN 96].
[6] Source: [THR 96].
[7] See http://all.net/contents/resume.html as well as http://www.iwar.org.uk/cip/resources/senate/economy/cohen~1.htm
[8] Source: [THR 96].
[9] http://www.rand.org/about/contacts/personal/libicki/

– 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 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 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 "information warfare" concept 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 is the cause of the different points of view on information warfare.

But 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

[10] Source: [THR 96].

disappearing? Will information technologies revolutionize societies to the point of 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 understand as much as possible what the United States mean 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, from 1992[12]. Subsequent evolutions, however, enhanced the concept before it finally found its place within the different American military doctrines.

[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*), Spillmann, K.R. & Krause, J. (Eds); see: http://www.isn.ethz.ch.

[12] DoD Directive TS-3600.1, December 21, 1992, “Information Warfare”.

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 – Information Operations[16]). Examining the content of this document with a comparative analysis of the official doctrine of the Joint Chiefs of Staff (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?

[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] [WOO 95].

[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. 136 pages. http://www.c4i.org/jp3_13.pdf.

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 Joint Chiefs of Staff approach (JP 3-13): the concept of counter-information and its two subsets of offensive counter-information and defensive 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

[18] Air Force Doctrine Document 2-5, August 5, 1998, http://www.dtic.mil/doctrine/jel/service_pubs/afd2_5.pdf.

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;

– 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 Joint Chiefs of Staff (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 Joint Chiefs of Staff. 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

[19] The abbreviation CNA will be used throughout this book.

[20] http://ics.leeds.ac.uk/papers/pmt/exhibits/469/jp3_13.pdf.

[21] http://www.ndu.edu/library/goldnich/99433pt1.pdf.

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.

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 own interests);

– psychological operations;

– electronic warfare;

– physical attack, destruction;

– special information operations;

– computer attacks.

[22] Page vii, JP 3-13.

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, 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