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/.

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.