Social Economic Debates
2015, Vol. 4, No. 1
ISSN 2360-1973; ISSN-L 2248-3837

The considerations on informational warfare

Associated Professor Agata Popescu PhD
Dimitrie Cantemir Christian University Department of Law
Email: av.agata@yahoo.com

Abstract: *Strictly military information warfare can be defined as all informational operations at tactical, operational and strategic level, in peacetime, crisis and conflict escalation, with the common goals of achieving or influencing certain targets. Information warfare has a military component, command and control warfare which has the following meaning according to NATO: "integrated use of all military capabilities including operations security, deception, psychological operations, electronic warfare and physical destruction, supported by all sources of intelligence, communications and information systems to deny access to information, influence, damaging or destroying command and control capability of an adversary, while their military capabilities are protected against similar actions".*

Key words: *information warfare, security operations, military capabilities.*

JEL Classification*: K32*

Introduction

Now the information warfare has become more attractive from a military point of view, given the increase in the number of targets vulnerable to cyber attacks and the increase of the need for them to be protected. In the new circumstances, it appears that no amount of information or the time will be a key factor in the political and military decision making. As such, during conflict situations opponents will have simultaneous access to enormous amounts of information, but one that will have the most accurate and complete information and will have an effective system for processing and protection will be the advantage.

Developments in recent years demonstrate clearly that we are witnessing the materialization of a new type of aggression, a new type of war, whose features and subtle manifestations far exceed the traditional classics.

The war of the XXI century will no longer have anything in common with the world wars that history has crossed. With the Cold War there are no longer required massive forces, their place being taken by flexible structures, agile, deployable, and able to intervene at short notice in any area of the globe. This was possible due technological progress, in particular, and the economic difficulties that states have encountered in recent years.

The core of the future type of war that will meet the requirements of this era is the concept of "war based on information" that is based on "the information age war theory and the principle of military planning and development of joint operational concepts and systems capabilities". This will change from the bottom up, the structure of the military forces and their culture, using experiments, means of transformation and the creation and dissemination of new knowledge and experiences.

Global networks and interest groups (virtual communities) occurred and were determined by the developing of communication and trading systems and the emergence and expansion of the Internet has changed and revised the concept

of community and how community members communicate with each other, while creating a cyberspace where different organizations share common interests (groups) or individuals.

If new information in the informational war was comparable to the previous and analyzed by different tools to achieve the best operational concepts in the information warfare solutions are limited to the use of information, algorithmic and with precise targets.

Therefore, information warfare requires constant technological upgrades to ensure continuous improvement in circuit information.

The Cold War period has seen a change in international relations and with them many concepts. A new landscape dominated both the concepts and the stakes, behind which lies most economic interests.

Information warfare is a concept so vast that it cannot be overlooked. Assuming that, from a certain point of view, modern disinformation itself is only one aspect of this war of information, we can appreciate that new types of wars, such as information warfare, electronic warfare, psychological warfare, media war became or will become increasingly used by the world's major powers but also by large corporations that have almost unlimited access to political decision makers (Cracsner, 2003).

The American Institute for Advanced Study of War Information (Institute for the Advanced Study of Information Warfare - IASIW) adopted a definition that some analysts in the field, George Stein, John Arquilla, David Ronfeldt, Martin Libicki, Winn Schwartau and others have few reserves and are looking to use it considering that it exhibits the best features of informational war (Cracsner, 2003).

According to them, information warfare is "*offensive and defensive use of information and information systems to exploit, corrupt or destroy adversary information and its information systems, while protecting their own information and information systems (Topor, 2006)*". By definition it is clear that *the American vision* of information warfare is similar to the concept of power, its measures are used to influence human life in general and the decisions they may take.

As a result of this definition, objectives and motivations of an actor that uses the information war as an instrument of control are elements in the information sphere.

So, if someone were to adopt the model would have thought a terrorist and war technology specific information could be more dangerous. This is unlikely, but far impossible. But, next big problem regarding the information war, which can have disastrous effects especially short term and which only a few years began to be given special attention, is terrorism information which has been allowed to emerge and expand due to the exponential growth of computer networks and also due to a lack of regulation by national legislatures and executives regarding the creation of mechanisms of protection against any kind of attack informatics computer. This increasing attention is shown in a recent press FBI (Federal Bereau of Investigation), which prepares becoming more adept to cope with the continuous increase in computer crime. Content cyber crime is very varied, being approached from different points of view in the literature (Buzatu, 2014).

Information warfare is the set of actions taken to achieve information superiority in support of national military strategy, affecting adversary information and information systems, maintaining and protecting their systems and information (U.S. Army land forces) (Strave, 2004).

Information warfare is "*any action intended to annihilate, exploit, damage or destruction of the enemy's information and information functions: ensuring its protection against such activities, taking advantage of their information functions*" (U.S. Air Force) [1].

Information warfare is fighting to collect information and to protect its own information, to suppress or neutralize information, to deceive and to detect deception, and to destroy and to protect the information destruction and its sources "(Wang and Li Fei Baocun -" Information Warfare ").

Information warfare may be a plurality of confliction states in information or technology information and will be engaged in different levels of future actions. Increased speed in information flows and data processing methods and virtual dependency information and information systems are inevitable requirements to ensure progress in all countries of the world (Ciobanu, 2005).

The characteristics of these types of war are different from the traditional ones. Information warfare means to use offensively and defensively information systems to exploit and destroy (Stavre, 2004).

Armed conflict is a political instrument and the military component – the army becomes a main aim to descourage, intimidate or sanction in a coercive way, but the main strategical actions will be carried out outside the are of command and control (Visscher Pierre, Neculau, 2001).

It will be mainly about distortioning of command but also inducing a favourable image by controlling the media[2].

The new types of war will be characterized by:

- New generations of weapons (intelligent) that will allow: anihilation and reducing the performances of the classical means;
- The classical relation between beligerents on the field *man-technical means-man*, will be radically changed and will take the form *technical means-technical means*;
- The new generations of weapons will dominate the classical ones and will make available new applications:
- Missile defense systems (missile shield).

Even today, sets of overlapping missile provide the best protection in the course of a ballistic missile attack. In the future, these instruments of death will be equipped with high performance sensors, which will enhance, at least theoretically, to the extent that efficiency will eliminate any threat with missiles (Topor, 2006). Romania in cooperation with NATO began in 2011 the work on a missile defense shield at the military base at Deveselu in Olt County, which should be completed by 2015.

- Weapons based on very powerful microwave frequencies - e-bombs, a weapon able to emit powerful beams of microwave that can "fry", literally, computers and electronics belonging to the enemy and military communication systems. This kind of weapon is an ingredient of many armed forces (Topor, 1989).
- Electric cannons;
- Nuclear missile;
- Active Denial System

[1] „Razboiul psihologic in conceptia principalelor state capitaliste'', Militara Publishing House Bucharest, 1972.
[2] Razboiul psihologic in conceptia principalelor state capitaliste" Militara Publishing House, Bucharest 1972.

- Scramjets;
- Space weapons;
- High power lasers;
- Autonomous weapons.

These are actually robotic vehicles, which are still in an experimental phase (some already entered production series such as drones used by the U.S. Air Force), from which is expected to destroy enemy troops plus military equipment from the ground and air without the risk of casualties (Hariu, 1994).

Perhaps the most spectacular informational warrior was Temujin (Genghis Khan), the creator of the Mongol Empire. This was accomplished by using skillful communication. Genghis Khan gathered intelligence with the intention to provide commanders who needed it as soon as possible[3].

Information warfare is all "actions at tactical, operational and strategic level, at peacetime, crisis, crisis and conflict escalation, using information resources to achieve their goals."

Information warfare is the set of "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while maintaining and protecting their systems and information."

Information warfare is a form of specific conflict specific for the beginning of this century and millennium since it answers some of the objections to both the politicians and the geo-strategic analysts and military planners about classical forms of ongoing conflicts (Popescu, 2003).

Lately it conveys both the notion of informational warfare and the war of the information age. Information age warfare uses information technology as a means of achieving savings in time and forces and as a means to streamline the actions. Information warfare uses information as a weapon and / or objective. The connection between the two phrases is that the information age technology allows direct manipulation of information available to the opponent.

Be it economic, financial, administrative, military, social, all these increasingly make use of larger systems to streamline work and increase productivity but neglect safety measures which are so necessary.

Rule of information is the main factor ensuring victory. In modern times information warfare will soon become as important as the land, sea, air and space. This is a permanent war, the one who owns and manages the information, and holds the power.

In conclusion, we can say that the new military concepts and technologies are developed and continually experimenting, allowing developed countries to enter the Information Era, with technological and doctrinal advantages difficult to achieve by other states. Against this background, the physiognomy of conflicts / wars will be completely revolutionize, the most significant advantage in the means of warfare will result in the quantity, quality, the high degree of processing and the use of information (Aquilla, 2010).

Acknowledging these aspect we may say that the advantages offered by development, doubled by military strategies and doctrine, military leaders, training and operativity will mean a real power.

In the last 2 years there were very dynamic and encripted threats and there is a risk that they increase.

[3] http:/bataiosu.wordpress.com/2011/01/07/topu-celor-mai-temute-10-armele-ale-viitorului/

References

Buzatu Nicoleta-Elena, *Evoluția incriminării fraudei informatice*, în *Crimes, Criminals and the New Criminal Codes: Assessing the Effectiveness of the Legal Response. In Honorem Professor George Antoniu*, Editura Accent, Cluj-Napoca, 2014.

Ciobanu Ionel, 2005, *Formele de baza ale razboiului informational.Corelarea si influenta acestora asupra desfasurarii actiunilor militare la nivel operativ*, U.N.Ap. Publishing House, Bucharest.

Cracsner C.E., 2003, *Elemente de psihologie militara*, Academia de Inalte Studii Militare Publishing House,Bucharest.

DeVisscher Pierre; Neculau A, 2001, *Dinamica grupului*, Polirom Publishing House

Golu P., 1989, *Fenomene si procese psihologice*, Stiintifica Enciclopedica Publishing House, Bucharest

Hariu C., 1994, *Protectia impotriva agresiunii psihologice*, Militara Publishing House, Bucharest

http:/bataiosu.wordpress.com/2011/01/07/topu-celor-mai-temute-10-armele-ale-viitorului

John Aquilla, 2010, *Noile reguli ale razboiului*, Foreign Policy Romania March/April 2010.

Stan Popescu, 2003, *Arta si puterea informatiilor*, Militara Publishing House, Bucharest

Strave Ion, 2004, *Reconstructia societatii romanesti prin audiovizual* ,Nemira Publishing House, Bucharest

Topor Sorin, 2006, *Razboiul Informational*, U.N.Ap. Publishing House, Bucharest