AARMS
Vol. 8, No. 2 (2009) 329–337

Connections between cyber warfare and information operations

ZSOLT HAIG

Miklós Zrínyi National Defence University, Budapest, Hungary

The article outlines the information-based warfare methods coming to the front in the up to date military operations. It explains cyberspace in a modern way, from a military point of view and it shows the way of reaching cyberspace superiority and the essence of cyber warfare in the information operations.

1. Methods of information-based warfare

In a society and economy networked with complex infocommunications systems we take care of almost all of our daily businesses in the net, we might fall into our own trap of advanced state. The government, economy structure, traffic network, power supply system etc. of a well networked and developed country can become paralyzed or can be limited in their operations. The health system can be limited as well, the public security can leave off and chaos can take the place of well organized order [1].

The defencelessness of the information society against non conventional threats can exemplify the terror attack and its impact of September 11th 2001. The industrial society – in which the economic, financial, and exchange systems were not as depending on the infocommunications networks – would not have felt the influence of this aggression so intensive; apart from the mental shock the physical and economic effects would have stayed restrained. Contrarily, in our networked world the collapse of the World Trade Center shocked the global economic system [2].

Let us figure what would happen if any alignment with harmful intentions, eventually a terror organization would set a physical or electronic attack – or a broadside of attacks – against the information society or against its important infrastructures. Through the information threats the networked infrastructures in a country with an advanced state of information technology, it's social, political, economical, and defence capacities would become very impressionable, through this its development would become strongly restrictable. This would intensify in case these attacks would accomplish in coordinated form of complex information attacks with the prudential selection of the targets.

Received: August 26, 2009

Address for correspondence:
ZSOLT HAIG
E-mail: haig.zsolt@zmne.hu

In the up to date military operations there is a fully novel theory that is called the effect based operations. Due to this principal an early, direct effect (first attack) can legitimately result further indirect harmful limiting influences that explains different scaled negative effects on the entire system. This new conception needs the adaptation of a holistic point of view. The essence of this is that in a system the components influence each other mutually [1]. This is even truer in an information society, where the different critical infrastructures, systems stay in close connection. The functioning of one depends on another one (etc.: the relation between the telecommunication or computer networks and the electric power supply systems).

In the defence sector the use of the information can be divided into two main areas. On one hand the information as the device of command and control in warfare, on the other hand the information as a “weapon” using so called non-kinetic energy in different information operations. Characteristic of both employments – in order to challenge information superiority over opposite forces – is the major scale utilization of the achievement of the information technology.

To achieve and secure the information superiority depends strictly on the quality of different sensors, on the speed of the command and control procedure, on the qualification of the executive forces and on the connection of the devices in a common network. All this means an up to date military command and control philosophy that is called Network Centric Warfare – using the NATO terminology Network Enabled Capability. Due to this the utilization of all resources is more effective in case the systems work connected; some resources are used divided, as if they exist independently, separately. The essence of this concept is that the participants of military operations can get easy access in real time, in the appropriate content and usable form of the necessary information in order to be able to accomplish their tasks. This new theory – integrating the sensor networks with the communication and information systems in a joint network – enlarges the combat capability [1].

Though to achieve information superiority it is not enough to apply most up to date military infocommunications systems in the command and control, or thus the utilization of the network enabled capabilities. To be able to reach and keep the information superiority it is absolutely necessary to defend these systems and to attack the similar systems of the opposite forces. Nowadays parallel to military operations on the conventional battlefield, there are also offensive and defensive information operations on the information battlefield.

Information operations are all the coordinated activities that influence decision-makers in support of political and military objectives by affecting other’s information, communication and information systems while exploiting and protecting one’s own similar systems [3]. The information operations – are also separately existing activities integrating and coordinating among complex information activities, which necessity and justification is given through the enlargement of the order of magnitude of the coordinated information operations.

In order to achieve the goals of the information operations it takes influences in the physical, information and cognitive dimension.

The information operations activities in the physical dimension mean the physical, destructive "Hard Kill" attacks against information infrastructures and infocommunications systems, as well as the physical defence of the own similar objects.

The information operations activities (data gathering, data processing, communication) in the information dimension mean the electronic so called "Soft Kill" attacks. On the other hand here belongs also the prevention of our own information processes from the opposite forces.

The information activities materializing in the cognitive dimension aim directly the human thinking – observation, perception, interpretation, opinion, supposition – with false, misleading information [1].

Within the confines of the information operations and the complex information attack tending against the entire information society can materialize in *total form* against civil and military targets as well as in a *focused way* against accentuated target groups or in a *selective form* against some critical infrastructures. The motivation factors of the threats can be the achievement of different political, economical, financial, military, social, cultural, industrial, ethnical, religious, regional, or personal goals. The threat against the information systems can change according to conflict situations, technical possibilities and due to motivations [4].

2. The novel interpretation of cyberspace

On the battlefield the various networked electronic systems apply that part of the information battlefield in which the information processes (electronic based data gathering, data processing, communication) materialize, respectively in which the operations against the electronic systems and the defence come true.

Due to civil terminology the overall definition of cyberspace is electronic devices and systems, computer networks, internet, telecommunication, satellite systems etc. and all supply, virtual space created of information that often is used for the virtual reality as well.

The military interpretation of cyberspace is different from the above. It is a lot wider. According to the document "National Military Strategy for Cyberspace Operations" of the USA: "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures” [5].

There are some military experts agreeing with the quoted definition: “…cyberspace is a very real, physical domain that is comprised of electronics and networked systems that use electromagnetic energy. Cyberspace exists across the other domains of air, land, sea, and space and connects these physical domains with the cognitive processes that use the data that is stored, modified, or exchanged” [6].

This dimension is extended through the military interpretation, and not only the functional environment of the computer networks are meant by that. On the battlefield nowadays there are such networks established of electronic devices (radios, radars, navigation devices, battlefield combat identification systems and computers) where it is very difficult to separate the system components. As along as we analyze the operations attacking these systems or their defence we have to interpret those by all means as complex system that has a common operational environment. On the battlefield these network systems (mostly as a mobile setup) use electromagnetic energy (in many cases the full frequency spectrum) to collect, store and transmit data and information. So far as these systems use the full frequency spectrum, through that it is possible to get access to them, to detect and to attack them.

The cyberspace is a place of warfare, equivalent and similar to land- air- sea- and space theatre. As you can characterize sea theatre on the sea surface or underwater operations so can you feature air theatre with operations in the air, the same way cyberspace can be characterized with networked electronic systems and with use of full frequency spectrum (Figure 1).

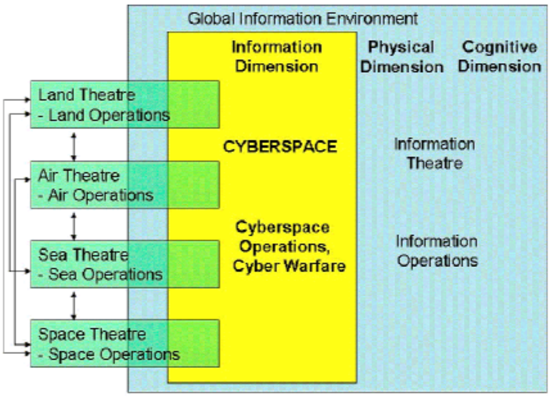
Global Information Environment
Information Dimension
Physical Dimension
Cognitive Dimension
Land Theatre - Land Operations
Air Theatre - Air Operations
Sea Theatre - Sea Operations
Space Theatre - Space Operations
CYBERSPACE
Cyberspace Operations, Cyber Warfare
Information Theatre
Information Operations

Figure 1. Interpretation of cyberspace

The vulnerability of the internet is nowadays well known. Due to this fact the security of the internet as a critical infrastructure is a very important task from a national security point of view, which has to be considered by the planning of protection of critical information infrastructures.

On the other hand in a country there are many networked systems working that are not connected to the internet. Most of the military command and control systems function as a separated, closed network; they do not have an immediate connection to the internet. If we intend to weaken the capability of the enemy's command and control systems we have to get access to their systems in an electronic way in cyberspace in the full frequency spectrum [6].

3. The cyber superiority

During the operations happening in the cyberspace creation and maintenance of the networked capabilities of the friendly forces as well as the weakening and destruction of the enemy is of major importance. All activities taking place in cyberspace aim to get and maintain cyber superiority. The cyber superiority is that part of information superiority that can be reached with various networked electronic devices, systems and computers. In order to achieve and maintain cyber superiority there are three equally important and close components to differentiate:

1. Various networked electronic systems secure the information of the current and the expected situation. On the one hand this means the electric based intelligence on the other hand the electronic processing, storage and transmitting of the information of the situation of the friendly forces. Thirdly it means the collecting, processing and transmitting battlefield environment data through electronic systems and devices.
2. Disruption and degradation of function of the enemy's electronic information systems. This means electronic attacks within the confines of electronic warfare, for example electronic jamming, electronic deception or destruction of the enemy's electronic devices and computers by electromagnetic pulse weapons (e-bomb). On the other hand within the confines of computer network operations it means the intrusion into the opposite forces' computer networks and through this busting, modifying databases and to generate program failures.
3. Exploitation and protection of the own information capabilities against the enemy's electronic attacks. This involves the maximal profiting of capabilities inherent in our own networked information systems, or rather the electronic protection and computer network defence of these.

According to the above definition of cyber superiority it connects to the information superiority, it is that part of it, which realizes in the information dimension, and its' attainment is ensured by the utilization of networked electronic systems on the battlefield, by defending our own systems and by attacking those of the opposite forces. Without cyber superiority it is not possible to achieve and maintain complete information superiority. This is the main reason why it is of capital importance in nowadays military operations.

4. Cyber warfare in the information operations

As we define cyber superiority as a part of information superiority, so its' achievement can be realized with cyber warfare within the information operations.

Considering the military interpretation of cyberspace, the cyberspace operations mean more than computer networked operations. We can count to this the following: interception of telecommunications network, jamming of those, different forms of electronic attack against radars and navigation systems, mapping of computer network, intrusion into them, blasting of databases and overload of servers or the operation against the Radio Controlled Improvised Explosive Devises (RCIED). These enumerated cyberspace operations are only some examples from the huge palette, that can be used against the enemy's electronic systems and computer networks.

Due to a novel approach the information operations can be divided into three separable parts. These three fields can be connected to the already mentioned three dimensions (physical, information and cognitive). These are the following:

- *kinetic warfare* that realizes in the physical dimension and it practically means the physical destruction, demolition and abuse of the components of the information infrastructures and infocommunications systems;
- *cognitive warfare*, which basically prevail in the mental dimension and it involves: military deception, operation security and psychological operations;
- *network warfare* that realizes in the information dimension and contains the following: electronic warfare and computer network operations [7].

As the all-source intelligence is the basic of the information operations so is the basic of cyber warfare the electronic based intelligence that is built on sensor networks. Accordingly the network warfare completed with the electronic based intelligence is nothing else than all the cyberspace operations, with other words: cyber warfare. (Figure 2).

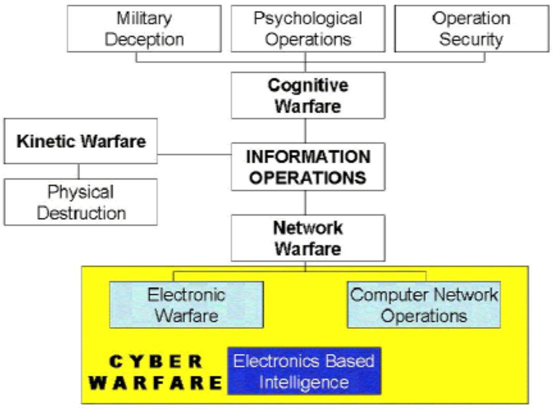

Figure 2. Connection of cyber warfare and information operations
[drawn by the author based on reference No. 7]

Cyber warfare can be offensive and defensive. The *offensive cyber warfare* has a double function: on one hand to detect, on other hand to influence and to destroy the networked information systems of the opposite forces. The attacker – avoiding the information security regulations – detects the communication systems, gets into the computer networks, gets access to various databases in order to gain useful information. He also can use jamming signals, misleading information, malicious software (malware) to modify, delete important information of the enemy or rather he can overload the system with misleading data [1].

The *defensive cyber warfare* tends to provide the access to the information and information-based processes in its' own networked information systems and to assure the effective use of these systems. It minimizes the vulnerability of its' own networked information systems and it lowers the unintentional interferences among them. The harmonized employment of the effective cyber defence makes it possible to defend our own networked information systems from the denial of service, from unauthorized access, from jamming and modification, etc. [1].

To establish cyber warfare capabilities the cyberspace attack series against Estonia in spring 2007 played probably a major role. The attacks can be related to the removal of some World War II monuments. This unique cyber attack in peace time shacked up also the authorized experts of the USA and those of the NATO. It has been assessed that even in peace it is possible to sustain a paralyzing attack against the internet that as well can be realizable as the intro-period of a conventional military operation.

According to the information warfare apprehension of Chinese military doctrine in order to achieve surprise and initial cyber superiority, cyberspace operations can be applied most effectively in the period of the first strike, more in its introducing part [8].

Because of the Estonian precedent – in order to create cyber attack capability and in the interest of assuring cyber defence – probably in a number of countries the development and shaping of cyber warfare forces will be started.

Conclusions

Through the implosive development of the information technology the role of information-based warfare in military operations will grow. The operation fields and ranges of military operations will flare further, the information battlefield showed up. The information battlefield is a matter of fact operation environment of the information operations in which all its three dimensions can be defined (physical-, information-, and cognitive dimension).

On the battlefield the different networked electronic systems use that field of the information battlefield in which the various electronic information processes (electronic based data gathering, data processing and communications) implement or rather where the attack against the electronic systems and their defence realize. This area of the information battlefield is called cyberspace. Cyberspace is a range where as well as all electronic devices operating in networked systems and the whole frequency range is used to store, transmit and modify data, respectively to attack and defence the systems working in the network. These latter activities carried out within the confines of cyber warfare in order to achieve and maintain cyber superiority.

Acknowledgement

The paper has been supported by the Bolyai János Research Scholarship of the Hungarian Academy of Science.

References

1. HAIG ZSOLT, VÁRHEGYI ISTVÁN: *Hadviselés az információs hadszíntéren*. Zrínyi Kiadó, Budapest, 2005. 286 p. ISBN: 963-327-391-9
2. *A hálózati társadalom sérülékenysége.* http://www.nato.int/docu/review/2002/issue2/hungarian/features2.html (downloaded: 27. 05. 2009.)
3. *Magyar Honvédség Összhaderőnemi Doktrína*. 2. kiadás. Magyar Honvédség kiadványa. MH DSZOFT kód: 11313. Budapest, 2007.

4. HAIG, ZSOLT, KOVÁCS, LÁSZLÓ, MAKKAY, IMRE, SEEBAUER, IMRE, VASS, SÁNDOR, VÁNYA, LÁSZLÓ: *Az információs társadalom veszélyforrásai*. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány. MEH Informatikai Kormánybiztosság, 2002
5. *National Military Strategy for Cyberspace Operations*. December 2006. http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (downloaded: 08. 09. 2009.)
6. FAHRENKRUG, DAVID T.: *Cyberspace Defined*. http://www.au.af.mil/au/archive/0209/Articles/CyberspaceDefined.html (downloaded: 24. 02. 2008.)
7. BOURQUE, JESSE: The Language of Engagement and the Influence Objective. *The Journal of Electronic Defense*. 30(1)1. (November 2007) 30–35 ISSN 192429X
8. MINNICK, WENDEL: Computer Attacks Form China Leave Many Questions. *Defense News*, August 13, 2007. p. 13. ISSN 0884-139X