ELECTRONIC WARFARE IN CYBERSPACE

Col. Prof. Zsolt HAIG, PhD, Ing
Faculty of Military Sciences and Officer Training
National University of Public Service, Budapest, Hungary

Abstract

The study outlines a new military operational environment consisting of the cyberspace and electromagnetic spectrum. It interprets the convergence between them and their common domain as well as shows the operations within it. Based on a US military concept, it describes the place and role of electronic warfare in cyberspace.

Keywords: Electronic warfare; Cyberspace; Electromagnetic spectrum; Cyber electromagnetic operations.

Introduction

Today we live in a networked world. The proliferation of information technologies is changing the way humans interact with each other and their environment. The mobility has an increased role in our rapid life. Mobile communication, mobile internet, navigation, etc. are taking place with wireless connection in the electromagnetic spectrum.

The modern armed forces operate in an increasingly wireless network-based world too. The armed forces use the electromagnetic spectrum in a wide range for communication, weapon control, intelligence, surveillance, navigation and force protection. Nowadays, there are numerous electronic devices with different types and designation on the battlefield. These devices work in this information- and electromagnetic environment, which makes it necessary to intensify the interoperability capabilities between them. The mass using of info-communications technologies on the battlefield requires military forces to operate in cyberspace and leverage the electromagnetic spectrum.

Electronic warfare

Electronic warfare plays a very important role in any military operations. All service components conduct and integrate electronic warfare into operations to support missions. Electronic warfare is integrated and synchronised with lethal fires in order to disrupt and increase the enemy's decision making reaction time. It supports:

- the force protection function by defending friendly electromagnetic communications and non-communications systems;
- the situation development, target development and acquisition, battle damage assessment, and force protection functions by identifying, locating, and exploiting enemy emitters;
- countermeasures against command and control by disrupting, degrading, and neutralising the effectiveness of the enemy's radios, radars, navigation, etc.

Electronic warfare supports friendly forces with different kinds of information about the enemy's electronic systems. Based on this information, the commander is able to recognise the organisations, capabilities and possible activities of the adversary in the close future. In addition, electronic warfare has methods, activities and devices to reduce the enemy's capabilities in the full electromagnetic spectrum. [1]

"Electronic warfare is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy". [2]
Electronic warfare consists of three main areas:

- electronic warfare support measures (or electronic warfare support);
- electronic countermeasures (or electronic attack) and
- electronic protection (see figure. 1).

Electronic warfare support measures consist of actions to search for, intercept, identify, and locate or localise sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Electronic warfare support measures provide information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support measures data can be used to produce signals intelligence (SIGINT), provide targeting for electronic or destructive attack, and produce measurement and signature intelligence (MASINT). [1] [2]

When considering the later detailed issues, signals intelligence must be mentioned in this context. The most important issue is that just like electronic warfare, signals intelligence also operates in the electromagnetic spectrum. Electronic warfare support measures and signals intelligence missions use the same resources and data collection methods. They differ in the purpose for the task, the detected information's intended use, the degree of analytical effort expended, the detail of information provided, and the timelines required.

Electronic countermeasures involve the use of electromagnetic energy, directed energy, or homing guidance weapons to attack electronic systems, facilities, or equipment with the intent of degrading, neutralising, or destroying enemy combat capability. It includes actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electronic deception, as well as employment of weapons that use either electromagnetic or directed energy to destroy the enemy's electronic assets. [1] [2]

Electronic countermeasures can be offensive or defensive. Offensive activities are generally conducted at the initiative of friendly forces. Examples include:

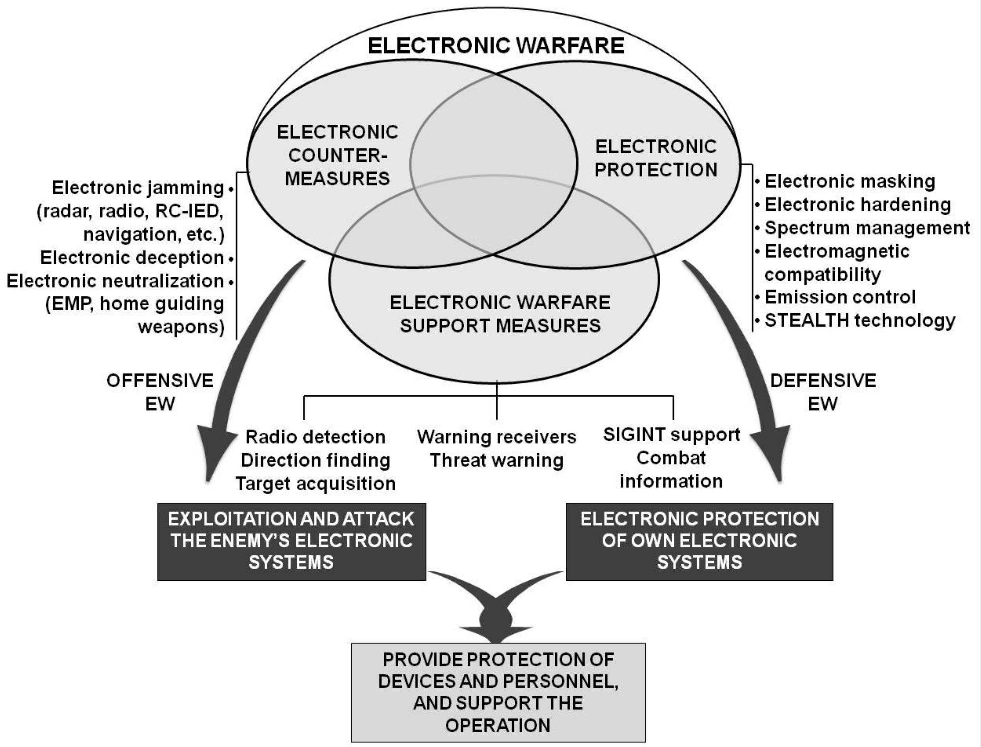
- jamming an enemy's radar or command and control systems;
- using antiradiation missiles to suppress an enemy's air defence system;
- using electronic deception techniques to confuse an enemy's intelligence, surveillance and reconnaissance (ISR) systems, and
- using directed energy weapons to disable an enemy's equipment or capability. [3]

Defensive electronic countermeasures protect personnel, facilities, capabilities and equipment. Examples include self-protection and force protection measures such as use of:

- expendables (e.g., chaffs, flares, and active decoys);
- radar jammers;
- towed decoys;
- infrared countermeasures systems, and
- counter radio controlled improvised explosive device (RC-IED) jammers. [3]

Electronic protection ensures the friendly use of the electromagnetic spectrum with special measures, techniques and activities. It consists of passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly unintended interference or enemy employment of electronic warfare that degrades, neutralises, or destroys friendly combat capability. [1] [2]

Electronic warfare employs many tactics, techniques and procedures to achieve its aim. These are illustrated in figure 1.


ELECTRONIC WARFARE
ELECTRONIC COUNTER-MEASURES
ELECTRONIC PROTECTION
ELECTRONIC WARFARE SUPPORT MEASURES
Electronic jamming • (radar, radio, RC-IED, navigation, etc.)
Electronic deception •
Electronic neutralization • (EMP, home guiding weapons)
• Electronic masking
• Electronic hardening
• Spectrum management
• Electromagnetic compatibility
• Emission control
• STEALTH technology
OFFENSIVE EW
DEFENSIVE EW
Radio detection
Direction finding
Target acquisition
Warning receivers
Threat warning
SIGINT support
Combat information
EXPLOITATION AND ATTACK THE ENEMY'S ELECTRONIC SYSTEMS
ELECTRONIC PROTECTION OF OWN ELECTRONIC SYSTEMS
PROVIDE PROTECTION OF DEVICES AND PERSONNEL, AND SUPPORT THE OPERATION

Source: edited by the author.

Figure 1. Electronic warfare: areas and capabilities

Convergence between cyberspace and electromagnetic spectrum

Using electromagnetic energy and operating in cyberspace are also essential to modern warfare. Military forces use wireless computer networks to coordinate operations, use air and ground sensors to detect and locate the enemy, use radios to communicate with each other and use electronic jammers to blind enemy radars or disrupt their communications. With wireless routers or tactical radios part of almost every computer network, cyberspace and the electromagnetic spectrum now form one continuous, coherent environment. The electromagnetic spectrum and cyberspace as a specific information environment are fundamental to military operations, so that we must treat it on a par with the traditional domains of land, sea, air, and space. Chief of Naval Operations, Admiral Greenert, stated this connection: „In fact, future conflicts will not be won simply by using the electromagnetic spectrum and cyberspace, they will be won within the electromagnetic spectrum and cyberspace." [4]

According to JP 3-13.1"the electromagnetic spectrum is the range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. [2] In a more detailed interpretation, "the entire electromagnetic spectrum, from the lowest to the highest frequency (longest to shortest wavelength), includes all radio waves (e.g., commercial radio and television, microwaves, radar), infrared radiation, visible light, ultraviolet radiation, X-rays, and gamma rays." [5]

The term cyberspace was first used by the author William Gibson in his book, Neuromancer. In this science-fiction novel, Gibson described cyberspace as the creation of a computer network that is often used for the virtual world or reality as well. Based on the Encyclopedia Britannica„ „cyberspace is an amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the internet's infrastructure." [6]

The military interpretation of cyberspace is different from the above mentioned civilian approach. Referring to the definition of the document "National Military Strategy for Cyberspace Operations" of the USA, cyberspace is "a domain characterised by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." [7]

The US Department of Defense modified this definition in 2008. "Cyberspace is 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." [8].

As it appears from the definitions, the military view expands the cyberspace and understands it by not only the internet and computer network, but other networked systems which manage information. While the first definition emphasises processes in cyberspace and stresses the electromagnetic spectrum, the second one focuses on the means operating in it, but does not emphasise the medium of the network contact. In a military environment, the maneuvering forces mostly use the electromagnetic spectrum for communication or to build up computer networks (e.g., tactical internet).

To summarise the above, we can accept Daniel Kuehl's definition: "Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infra-structures." [9]

An important feature of cyberspace is that networked info-communication systems operate in it using electromagnetic spectrum and/or wired connection. Different electronic information management processes (electronic data gathering, data processing, data storage, communication) are going on in these systems. The stress is on the network, but it is necessary to note that not all devices that operate in the electromagnetic spectrum are in the network in the battlespace. There are stand alone devices too (e.g., stand alone unattended sensors, expendable jammers, radio controlled improvised explosion devices, etc.). So cyberspace is not equal to the electromagnetic spectrum, it can only be applied to networked electronic systems. As a result, the two domains - namely the cyberspace and electromagnetic spectrum - approach each other and there is a convergence between them.

Cyberspace exists across the other domains of land, sea, air, and space. It is the use of electronic technologies to create cyberspace and use the electromagnetic spectrum that sets cyberspace apart from the other domains, and which makes cyberspace unique. [10] One main characteristic of cyberspace is that it cannot exist without being able to exploit the naturally existing electromagnetic spectrum. Without it, not only would millions of info-communications technologies (ICT) be unable to communicate with each other, but the info-communications technologies themselves would be unable to function. Moreover, info-communications networks are also dependent upon the electromagnetic spectrum for their essential connectivity via radio frequency. [11]

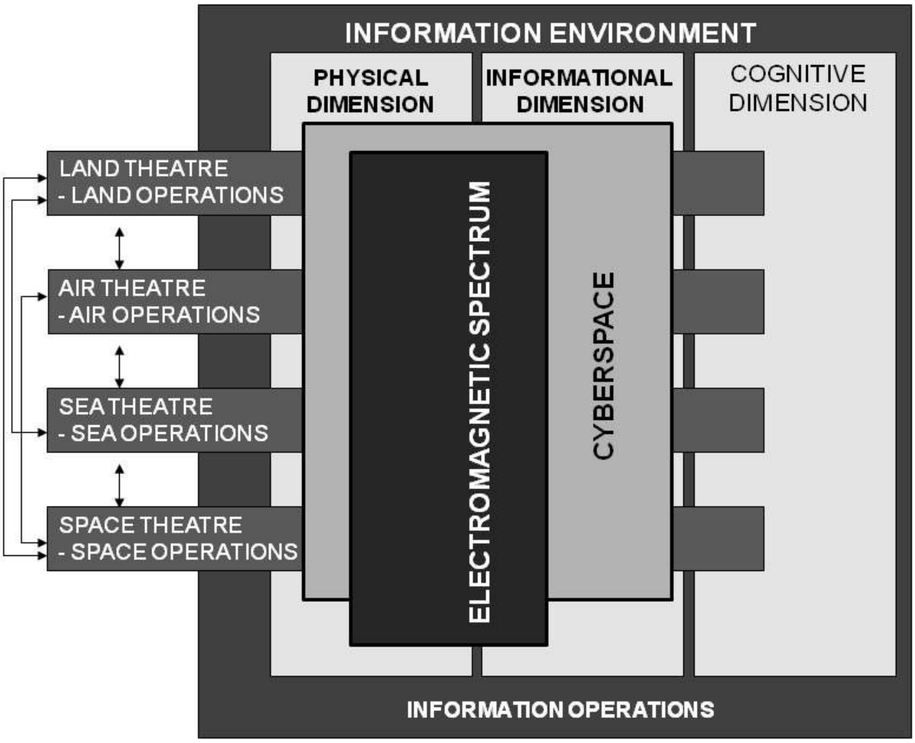
On the battlefield nowadays, such networks of electronic devices (radios, radars, navigation devices, battlefield combat identification systems and computers) are established where it is very difficult to separate the system components. We have to interpret these by all means as a complex system that has a common operational environment. On the battlefield these network systems (mostly as a mobile setup) use electromagnetic energy to collect, store and transmit data and information. So the electromagnetic spectrum receives its place in the military interpretation of the cyberspace together with the virtual space created by wired networks.

Cyberspace and the electromagnetic spectrum are part of the information environment. „The information environment is defined as the virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems." [12] The information environment has three interrelated dimensions:

- physical dimension;
- informational dimension and
- cognitive dimension.

The information environment is the arena of information operations, in which information based activities are conducted in the physical-, informational- and cognitive dimensions. The electromagnetic spectrum and cyberspace reside within the physical and informational dimensions of the information environment.

The cyberspace and electromagnetic spectrum are a place of warfare, equivalent and similar to the land- air- sea- and space theatre. As you can characterise the sea theatre on the sea surface- or underwater operations - so you can feature the air theatre with operations in the air, the same way cyberspace can be characterised with networked electronic systems and with use of the electromagnetic spectrum. (figure 2.)



Source: edited by the author.

Figure 2. Interpretation of cyberspace and electromagnetic spectrum

There is an overlap between the cyberspace and electromagnetic spectrum and it results in multidiscipline effects. The cyberspace and electromagnetic spectrum create a common operational environment that could be named as the cyber electromagnetic domain. The cyber electromagnetic domain is not meant to equate the terms cyberspace and electromagnetic spectrum, but rather to highlight that there is significant overlap between them and future technological development is likely to increase this convergence.

In this domain, harmonised, coordinated and integrated information technical activities take place. These activities could be called cyber electromagnetic operations.

Cyber electromagnetic operations

US military experts recognised the force multiplier role of the common cyber and electromagnetic domain and the synchronised information technical activities within it. Based on this idea, a new operational concept was developed in the FM 3-38 Cyber electromagnetic activities doctrine, which was issued in February 2014.

"Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system." [13]

The essential cyber electromagnetic activity is to integrate and synchronise the functions and capabilities of cyberspace operations, electronic warfare, and spectrum management operations to produce complementary and reinforcing effects. The uncoordinated activities may result in conflicts and mutual interference between them and with other entities that use the electromagnetic spectrum.

Cyber electromagnetic activities consist of:
- cyberspace operations;
- electronic warfare and
- spectrum management operations. [13]

As we can see, the cyber electromagnetic operations include another two capabilities in addition to the electronic warfare, which was shown earlier. "Cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. Cyberspace operations consist of three functions: offensive cyberspace operations, defensive cyberspace operations, and Department of Defense information network operations." [13]

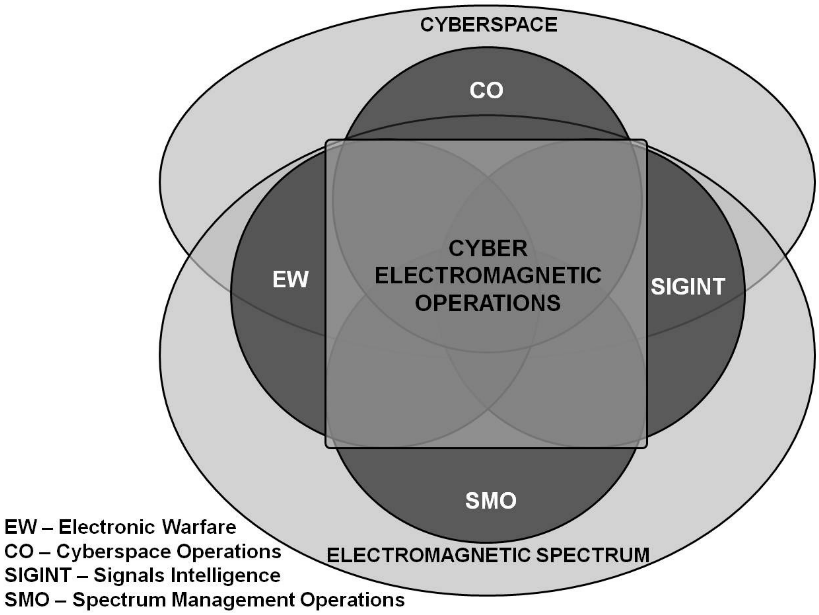
Earlier, the cyberspace operation was slightly equal with computer network operations. According to this doctrine, the cyberspace operations are more than computer network operations. These operations consist of not only computer network exploitation, computer network attack and computer network defence, but networked information management activities (collection, storage, processing, distribution) are part of them too.

“Spectrum management operations are the interrelated functions of spectrum management, frequency assignment, host-nation coordination, and policy that enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations.” [13]

Spectrum management operations are emphasised in the doctrine as the interrelated functions of spectrum management, frequency assignment, host-nation coordination, and policy. These functions together enable the planning, management, and execution of operations within the electromagnetic spectrum during all phases of military operations. In addition, careful frequency management helps to avoid frequency confliction or unintended electromagnetic interference. In a wider interpretation, spectrum management operations together with electronic warfare form the electromagnetic spectrum operations (EMSO). [13]

Referring to the close connection between electronic warfare and signals intelligence – which was mentioned in the first part of this paper – it would be necessary to consider signals intelligence capabilities in the common cyber electromagnetic domain. Based on the US Army’s cyber electromagnetic activities concept and further thinking about it, the cyber electromagnetic operations include the signals intelligence too as another element of the electromagnetic spectrum operations. Considering the electronic warfare and signals intelligence networked constraints, the cyber electromagnetic operations consist of:

- cyberspace operations;
- electronic warfare;
- signals intelligence and
- spectrum management operations. (figure 3).


CYBERSPACE
CO
EW
CYBER ELECTROMAGNETIC OPERATIONS
SIGINT
SMO
ELECTROMAGNETIC SPECTRUM
EW – Electronic Warfare
CO – Cyberspace Operations
SIGINT – Signals Intelligence
SMO – Spectrum Management Operations

Source: based on [13] edited by the author.

Figure 3. Cyber electromagnetic operations

We should emphasise that while cyberspace operations are fully part of the cyber electromagnetic operations, the electronic warfare and signals intelligence are interpreted in the networked info-communications environment, as areas of the cyber-electromagnetic operations.

The fundamental aim of the cyber electromagnetic operations is to ensure use of the friendly networked electronic info-communications systems and the processes in them, and to detect, reduce and degrade the adversary's similar capabilities. These operations can be offensive and defensive.

The offensive cyber electromagnetic operations have a double function: on one hand to detect, on the other to influence and destroy the networked information systems of the opposite forces. The attacker, using mostly passive techniques and sidestepping the information security regulations, detects the communication systems, gets into the computer networks, and gets access to databases in order to gain useful information. He also can use jamming signals, misleading information, and malicious software (malware) to modify, delete important information of the enemy or rather he can overload the system with misleading data.

The defensive cyber electromagnetic operations tend to ensure access to the information and information based processes in our networked info-communication systems and to assure the effective use of these (systems). They minimise the vulnerability of our systems and they lower the unintentional interferences among them. The harmonised adaptation of effective defence makes it possible to protect our own networked info-communication systems from the denial of service, from unauthorised access, from jamming and modification, etc.

As we mentioned earlier, not all electronic devices work in network. Consequently, we understand only those tactics, techniques and procedures of electronic warfare and signals intelligence among these common cyber electromagnetic operations, which are used against the enemy's networked info-communications systems, or to protect friendly forces' similar systems. So, for example, detection of a radio communications network, or jamming it, as well as jamming the radio channels of a battlefield computer network are some examples of electronic warfare in cyber electromagnetic operations. But e.g. jamming a receiver of a radio controlled by an improvised electronic device is not part of electronic warfare in cyber electromagnetic operations.

Conclusions

Cyberspace and the electromagnetic spectrum are part of modern military operations. The military forces use many types of networked electronic devices and info-communications systems on the battlefield. Using these networked systems is necessary to achieve operational superiority.

The electronic warfare in the electromagnetic spectrum contributes to achieving information superiority and success of military operations by using offensive and defensive tactics, techniques and procedures.

The networked electronic info-communications systems work in the cyberspace and electromagnetic spectrum, and they create an overlapped common military operational environment. This environment is the cyber electromagnetic domain. In this domain, synchronised and integrated cyber electromagnetic operations are conducted. The electronic warfare that is used against the enemy's networked info-communications systems, or to protect our similar systems, is the main capability of these operations.

References

[1] Kovács, L.: Electronic warfare and the asymmetric challenges. in: Bolyai Szemle 2009. no. 3., 135-151 pp., ISSN 1416-1443

[2] JP 3-13.1 Electronic warfare. 08 February 2012. Joint Chief of Staff

[3] FM 3-36 Electronic warfare. 09 November 2012. Headquarters, Department of the Army

[4] Greenert J.: Wireless cyberwar, the EM spectrum, and the changing Navy. http://breakingdefense.com/2013/04/adm-greenert-wireless-cyber-em-spectrum-changing-navy/ (online, cit. 2015-01-10)

[5] Electromagnetic spectrum. http://www.britannica.com/EBchecked/topic/183297/electromagnetic-spectrum (online, cit. 2015-01-10)

[6] Cyberspce. http://www.britannica.com/EBchecked/topic/147819/cyberspace (online, cit. 2015-01-10)

[7] The National Military Strategy for Cyberspace Operations. December 2006., Chairman of the Joint Chiefs of Staff. http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf (online, cit. 2015-01-10)

[8] JP 1-02 Department of Defense Dictionary of Military and Associated Terms. 08 November 2010. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (online, cit. 2015-01-10)

[9] Kuehl, D.: From Cyberspace to Cyberpower: Defining the Problem. in: Cyberpower and National Security. ed. Kramer, F. D. et al., 2009., 24-43 pp. ISBN-10: 1597974234

[10] Schreier, F.: On cyberwarfare. DCAF Horizon 2015 Working Paper No. 7 2012., 133 p. http://www.dcaf.ch/content/download/67316/1025687/file/OnCyberwarfare-Schreier.pdf (online, cit. 2015-01-10)

[11] David J. Lonsdale, The Nature of War in the Information Age: Clausewitzian Future, 2004., 269 p. ISBN-10: 0714684295

[12] AJP-3.10 Allied Joint Doctrine for Information Operations. November 2009. NATO Standardization Agency

[13] FM 3-38 Cyber electromagnetic activities. 12 February 2012. Headquarters, Department of the Army