Iulian Boldea, Dumitru-Mircea Buda (Editors)
CONVERGENT DISCOURSES. Exploring the Contexts of Communication
Arhipelag XXI Press, Tîrgu Mureș, 2016
ISBN: 978-606-8624-17-4
Section: Communication, Public Relations and Journalism

CONSIDERATIONS ON CYBER WARFARE

George Antoniu Pișleag
Assist. Prof., PhD, National Intelligence Academy

Abstract: The virtual space and its basic infrastructure is vulnerable to a wide range of risks and hazards resulting from physical and cyber threats. Sophisticated cyber actors and the nation-states exploit vulnerabilities in order to extract information and money and they are developing capabilities to disrupt, destroy or threaten the provision of essential services. A number of traditional crimes are now committed through cyberspace. These include production and distribution of controlled materials, financial fraud, violations of intellectual property and other crimes, which all have substantial human and economic consequences.

Keywords: cyberspace; cyber security; cyber-society; cyber warfare; security

The new information technologies are expanding and becoming more integrated into the everyday life. It is expected that almost all areas of human activity will be dependent on and influenced by internet, which has “now become a reference component of the social space. Generically called the Internet, the computer network extended at planetary level represents a reliable support for a new form of social expression: cyber-society”[1]. Cyberspace, however, was gradually assimilated to the Internet phenomenon to which there were attached new social dimensions, “a new universe, a parallel universe created and sustained by the world of computers and communication lines. It is a new stage, a new and irresistible development for developing the culture and human activity under the sign of technology.”[2] These technologies have fascinated the users “and overcoming the concrete geographical boundaries of the communication process with the help of the computers and the network connections, it has thus represented a shift from a real space to a virtual one, known as the cyberspace”.[3]

In order to develop a definition of cyber warfare, we need to relate to specific actions, the involved actors, intentions and objectives and last but not least the context. The developments in information technology opened up more and more obvious possibilities so that every military conflict contains also the cyber warfare component. The cyber operations understood as “the ability to manipulate from the distance the computer networks, thus

[1] http://www.mes05.home.ro/6_SpatiiVirtuale.htm. Beyond the utopian optimistic anticipations that associated it with an ideal and inevitable direction of the evolution of the contemporary society or the negative approaches which refuse in principle the idea of virtual, the cyber society exists and develops at a rapid pace. Starting with the e-mail (e.g. “electronic mail” = e-mail) invented in 1971 by Ray Tomlinson, the prefix "e" (English “Electronic”) has registered an extensive semantic association covering a wide range of areas, activities and even geographic areas (such as eEurope). The attributes “electronic”, “virtual”, “cyber”, “online” and the phrase “mediated by Computer” are already implemented to an extensive array of components or social processes: virtual society (or cyber-society), virtual communities, virtual groups, virtual classrooms, social relationships mediated by computer interactions, virtual, computer-mediated communication, electronic commerce (e-commerce), online government, e-health, electronic signature (e-signature), online media, electronic journals (e-journals), (e-gifts), electronic greeting cards (e-greetings), the list can go on. It remains to be discussed how many of them are currently available and functional, as the temptation of “virtualization” is quite high.

[2] Michael Benedikt, Cyberspace: First Steps, Cambridge, The MIT Press, 1991.

[3] http://www.mes05.home.ro/6_SpatiiVirtuale.htm.

creating a new military capability. The internet and computers provide computer tools and techniques used to influence, constraint and even attacks. The military will use cyber-attacks to disrupt the command and control, in order to manipulate the software, affecting the performance of weapons and producing political or psychological effects"[4].

It is considered more and more by analysts, soldiers, that cyberspace is the fifth domain of warfare along with the land, sea, air and space operations, which led to the growth and expansion of the debate on cyber warfare. Terms such as "cyber security, cyber-attack, cybercrime, cyber warfare and cyber terrorism have entered into public discourse; however, there is no consensus on their definitions, making it difficult to create a conceptual framework in which the international relations and agreements related to cyberspace can be developed."[5] Given the inter-connected nature of cyberspace, it requires that the "States should cooperate to ensure the cyber security through international mechanisms, common standards, security standards, ways of adapting and strengthening the existing regulations for the enforcement of the law and the information exchange. The events demonstrate that cyber threats, cybercrime, cyber terrorism know no boundaries."[6]

The ease of accessing the Internet, the anonymous communication and "the asymmetries in the vulnerabilities which enable the smaller actors to have a greater capacity to exercise the hard and soft power, in the cyberspace than in more traditional areas of the political world"[7] by which it can cause ethical, moral, physical, some criminal damage.
The cyber threats, in general, under the form of crime, terrorism or military cyber-attacks are increasing and they have behind them, terrorist groups or states leading to an aggressive policy. Regardless of the players involved in such actions, they have exchanging, amorphous, ambiguous and fluid identities. This ambiguity "is a state of reality in cyberspace. The problem of assigning the identity of these categories of actors is really a challenge."[8] At the same time, the military cyber-attacks can be executed by non-state actors, openly or concealed, which may take back the state. The terminology used for such actions is not always complete and adequate for all activities, especially those of cybercrime. Thus, the military definition of cyber-attacks is largely covered by "the term Computer Network Operations which include Computer Network Attacks (offensive operations designed to disrupt, degrade or destroy information in the residence computers and computer networks), Computer Network exploitation (espionage actions facilitating the collection of information via computer networks and exploiting data gathered from target systems or information about the opponent) and Computer Network Defense".[9]

According to the specialized literature[10], the cyber-attacks are classified into three levels:
- Level 1 - network wars which represent mostly the cyber-attacks, most of all cybercrime activities and cyber-espionage (which may have the cyber warfare dimension);

[4] Charles G. Billo, Welton Chang, Cyber warfare, An analysis of the means and motivations of selected nation states, Institute for Security Technology Studies, Dormtmouth College, 2004, p. 32.
[5] Cyber defence in the EU, Preparing for cyber warfare?.
[6] United Nations Institute for Disarmament Research Geneva, Switzerland, The Cyber Index International Security Trends and Realities, 2013, p.114.
[7] J.S. Nye, Jr., Cyber Power, Belfer Center for Science and International Affairs, 2010, p. 1. http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.
[8] Directorate – General for External Policies of the Union, Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the UE, April 2011, p. 16.
[9] Ibidem, p. 7.
[10] Directorate – General for External Policies of the Union, Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the UE, April 2011, p. 16.

- Level 2 – the cyber-attack, damage, disable or interruption of an IT system with kinetic effects;
- Level 3 - hidden attacks (malicious manipulation) planned, orchestrated which may generate widespread damage.

A highly profitable enterprise is represented by cybercrime whose structure and nature are extremely diverse and difficult to isolate. The globalism of the Internet offers also the manifestation of activism (cyber-mob) and cyber terrorism, representing the conventional activities in supporting terrorism.

Cyber warfare is a "sub-section of the informational war.[11] As part of this broader concept, which aims at influencing the behavior and capabilities of opponent's leadership at the political and military level and/or to influence the attitude of the civilian population in the operating theaters or target countries, the cyber warfare includes only activities conducted to this end in the cyberspace".[12] The main difference between cyber terrorism and cyber warfare lies in the nature of the state, non-state or substate actors. The features of cyber warfare may be summarized as: real; it can destroy a modern nation; it occurs with extremely high speed; It is global; it goes beyond the usual battlefield; by its nature it continues to blur the difference between peace and war and it adds a new dimension of dangerous instability; cyber security requires active strategies; it became a conceptual tool to express different levels of inter-state conflicts through and in the cyberspace.

Cyber security became a strategic concept, being at the beginning more a technical discipline. It is also a product of security's concerns "that shapes the international agenda and that is a difficult challenge for foreign policy and international security."[13]

Cyberspace includes physical infrastructure consisting of integrated circuits, processing and storage devices, communication infrastructure, fiber optic cables, transmitters, receivers, power, software as a variety of systems based on programs, instruction, information. Such physical components are based on the hardware and software. Another component of this area consists of the data that they contain and that produce information. Based on these "structural and organizational properties, the cyberspace is a highly complex process and it is subject to frequent changes."[14] It can be said that cyberspace includes those "interconnected infrastructure networks of the information technology, including the Internet, telecommunications networks, computer and embedded computing systems"[15] and the virtual environment includes those "stored data and information processed by computers and transferred by these networks."[16] All these approaches only remove the conceptual difficulties of the term cyberspace and provide a correct understanding of the processes occurring in this computerized world and their interaction with national security issues.

Connecting with national security issues is based on the particular properties of the virtual space that are generated from national security threats and challenges through what the

[11] Actions taken to achieve information superiority by affecting the information of the adversary, information-based processes, information systems and computer-based networks while protecting their own information, information processes, information systems and computer networks.

[12] Dan Plăvițu, Războiul cibernetic – de la posibilitate la realitate/Cyberwar - from possibility to reality. Direcția Generală de Informații a Apărării/The General Directorate of Information for Defense. *Revista Infosfera/Infosphere Journal*, IIIrd year, no. 2/2011, p. 3.

[13] James A. Lewis, Cyber War: Definitions, deterrence and foreign policy. *Center for Strategic and International Studies (CSIS)*, 2015, p. 8.

[14] Lior Tabansky, Basic Concepts in Cyber Warfare. *Military and Strategic Affairs*, vol. III, no. 1, May 2012, p. 78.

[15] Ibidem.

[16] Ibidem.

cyber weapons represent (offensive weapons under different types of malware - viruses, worms, Trojan horses, logic bombs, etc.; dual-use instruments - network monitoring, scanning, penetration, encryption, camouflage, etc.; defensive tools – firewall, recovery systems in case of disaster. Amid the cyberspace novelty, the lack of correlation of some concepts with real physical space, defining cyber warfare becomes somewhat difficult to formulate.

Hostile activities in various forms, cybercrime, espionage, recruitment, activism, radicalization, propaganda, manipulation, attacks, etc. in cyberspace can be classified according to the types of activities (actions) taken and the caused damages.

If the social global space is based on generally valid principles determined by natural, biological, psychological and societal conditionings, the cyberspace goes beyond proximity boundaries in space and it expands globally of the use of various means for information processing and communication, which has led to considering the new issues influencing the security of the global cyberspace. The development of information technology has made it to become a major element of national power. It is increasingly obvious that under the intellectual and financial aspect, the capital is invested more to improve the cyber warfare content than for prevention.

The concept of cyber warfare has become more commonly used to refer to any conflict in cyberspace, with an international dimension, from cyber vandalism (cyber hacktivism), cybercrime to cyber espionage.

CyberPower represents the power based on the information resources as the amount of strategic effects generated by cybernetic operations in and from cyber space, the ability to influence and use the cyberspace to create advantages and events in other operational environments.

Regarding the “cyber warfare it is often treated not only as something new in the technical and military landscape, but also as something that exists unprecedentedly in the military affairs”[17]. Due to its nature, the cybernetic domain became an environment where diverse strategic cultures can manifest. For example, the “Russian strategic culture focuses on cyber warfare as a political activity for shaping the political outcomes by changing political perceptions of opponents who would respond better to Russian interests.”[18] At the moment, there are no rules of international law governing the cyber conflicts, and also no international agreement to that effect. However, the concerns at international level were recorded by the Group of Governmental Experts[19] established under the Resolution 68/243 of the UN which requested to the Secretary General to create a new GGE, who will report to the General Assembly in 2015.

The group agreed on a consensus report substantially in June 2015 (A/70/174) on standards, rules or principles of responsible behavior of states in cyber-sphere, and measures of confidence-building, international cooperation and capacity building which could have wider application at the level of all states. Also it has been established the way of applying the international law in using information and communication technologies. In the report it states that “few technologies have been as strong as in information and communication technologies for reshaping economies, societies and international relations. The cyberspace touches every

[17] Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015, p. 29.
[18] Ibidem, p. 36.
[19] GGE is formed of experts of Belarus, Brazil, China, Columbia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russian Federation, Spain, Great Britain and USA.

aspect of our lives. The benefits are enormous, but they do not come without risks. The stability and security of cyberspace can be achieved only through international cooperation and this cooperation should be the foundation of international law and the UN Charter principles."[20] The report includes recommendations drawn up in the form of restrictive rules and principles setting the good practice and the positive rights for international security.

The ambiguity continues on the implementation of the UN Charter "it serves the interests of Russia and China for not creating legitimacy and reasons for preferring the concept of conflict of information instead of cyber conflict."[21]

Unlike classical propaganda, the information warfare by the globality of the Internet reaches a worldwide audience through the narrative and dynamic dimension through which the diaspora, foreign audience can interact with the current events in real time using online platforms. Beyond the difficulty of defining cyber warfare, it remains still the certainty that it is a constant threat as a state of conflict, even if violence does not manifests itself directly and openly.

BIBLIOGRAPHY:

Benedikt, Michael, *Cyberspace: First Steps*, Cambridge, The MIT Press, 1991 Charles G. Billo, Welton Chang, *Cyber warfare, An analysis of the means and motivations of selected nation states*, Institute for Security Technology Studies, Dormtmouth College, 2004.

Geers, Kenneth (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015.

Lewis, James A., *Cyber War: Definitions, deterrence and foreign policy*, Center for Strategic and International Studies (CSIS), 2015.

Nye, J.S. Jr., *Cyber Power*, Belfer Center for Science and International Affairs, 2010.

Plăvițu, Dan, Războiul cibernetic – de la posibilitate la realitate/Cyberwar - from possibility to reality. Direcția Generală de Informații a Apărării/The General Directorate of Information for Defense. *Revista Infosfera/Infosphere Journal*, III^rd year, no. 2/2011.

Tabansky, Lior, *Basic Concepts in Cyber Warfare*, Military and Strategic Affairs, vol. III, no. 1, May 2012.

United Nations Institute for Disarmament Research Geneva, Switzerland, *The Cyber Index International Security Trends and Realities*, 2013.

Directorate – General for External Policies of the Union, *Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the UE*, April 2011.

Online Sources

http://www.mes05.home.ro/6_SpatiiVirtuale.htm.

http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf.

https://www.un.org/disarmament/topics/informationsecurity/.

[20] https://www.un.org/disarmament/topics/informationsecurity/.

[21] Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCD COE Publications, Tallinn 2015, p. 43.