The dimensions of CYBER WARFARE in the sino-russian space

Adrian Victor VEVERA
National Institute for Research and Development in Informatics - ICI Bucharest
Mareșal Alexandru Averescu Bvd, Nr. 8-10, Bucharest, Romania
victor.vevera@ici.ro

Ella Magdalena CIUPERCĂ
National Institute for Research and Development in Informatics - ICI Bucharest
Mareșal Alexandru Averescu Bvd, Nr. 8-10, Bucharest, Romania
ella.ciuperca@ici.ro

Abstract: Cyber warfare is an indisputable reality of our day. In this paper we have chosen to present some distinctive elements of the Chinese and Russian strategy, as essential competitors of the European Union. For this purpose, we studied the main characteristics of the strategy and hostile operations attributed to China and Russia. Despite the official statements where they define themselves as victims of cyber operations, Russia and China have defined clear ways of cyber intervention on the enemy / competing states.
Keywords: cyber war, cyber security, cyber attack, hostile cyber operations

INTRODUCTION

The desire to bring light to the way army should approache the problem of cyber warfare is necessary to be based on a correct understanding of the used concepts, on the identification of the actors and on the forces facing them, on the principles (if any) that govern this type of war.

Probably the most important innovation, when discussing cyber warfare, is the space where it takes place. First of all, the transition from physical to online space meant a need for a paradigm shift in the minds of those designated to defend national security. Knowledge of military maps, military strategy and how conventional weapons can be used in the best way has not been enough. The new type of cybernetic military man did not need special physical training, nor a thorough knowledge of military principles or the theory regarding national security and international relations. He only had to master cybernetic space.

CYBERNETIC SPACE

The attempt to clarify what cyber space means puts us in a position to identify at least one widely used contemporary bias. Currently the cyber space is regarded as the whole of the computer mediated elements, especially everything related to the world wide web.

And yet the discussion of cyber space should be dated long before, since the advent of the telegraph, in 1886 (Kremling and Sharp Parker, 2018, 31). Then, for the first time in history, people were able to communicate at very long distances in a binary manner of expression.

Paradoxically, the term cybernetic space was not imposed by engineers or computer scientists, but by a Canadian-born American writer William Ford

Gibson, who managed to describe the informational era in 1982 in his work the Burning Chrome long before the Internet came out. Subsequently, the emergence of the World Wide Web forced the use of this term in everyday life.

Despite its ubiquity, cybernetic space has been defined in different ways, depending on the authors' specific approaches and interests. In the National Strategy to secure cyber space (2003), the United States defined cybernetic space as „the nervous system of these critical national infrastructures - the control system of our country. The cyber space includes hundreds of thousands of interconnected computers, servers, routers, switches and fiber optic cables, which make our critical infrastructure work."

Reputed American scientist Daniel T. Kuehl (2009) refers to cybernetic space as „an operational domain whose distinctive and unique character is framed by the use of electronic and electromagnetic spectrum to create, store, modify, change and exploit information through systems. IT and interconnected communications and associated infrastructures".

The European Union has been interested in defining the cybernetic space, having as its first objective the possibility of introducing elements that can facilitate its defense and security. European Union is a complex unit, in which a multitude of socio-political factors of extremely different origins, specific for a heterogeneous cultural, social, political, historical and economic background coexist. Thus, the European Union has to overcome difficulties inherent in the legislative harmonization and regional integration.

Although in the official documents and in the specialized literature Russia does not pay much attention to the definition of the cybernetic space, it has not been delayed in establishing itself in this new territory. In general, the characteristics of cyber space are treated simultaneously with its specific vulnerabilities and risks. For example, in the Doctrine of the Russian Federation of Information Security (2010, 2014, apud Darczewska, 2016, 11), information security and information weapons are considered tools that can be used to achieve state interests.

A particular feature of the Russian approach is the emphasis placed on the psychological effects determined by the actions taken in cybernetic space. Therefore, in Russian doctrine cybernetic space is considered an important dimension of the informational space, defined as "the sphere of activities related to modeling, creating, transmitting, using and storing information, which influence the consciousness at the individual and social level, as well as the information infrastructures and the information itself" (Darczewska, 2016, 11).

From the Russian point of view, the informational threats must be treated responsibly, their effects being predominantly psychological. Regarding their fight and prevention, there is an emphasis on the role of technology that must double the efforts made in the psychological dimension. Therefore, in accordance with Russian doctrine, elements specific to propaganda operations are obviously taken into consideration and treated with the big care in official Russian documents and policies, both for the purpose of designing offensive operations and for the defensive ones. According to the Russian doctrine, the Russian cybernetic space is protected against the competitive models of political, economic, social and cultural development (Darczewska, 2016, 13).

In the **Cyber Security Strategy of Romania**, the cyber space is considered to be „the virtual environment, generated by the cyber infrastructures, including the information content processed, stored or transmitted, as well as the actions carried out by users in it" (2013, 7).

The national approach of national security strongly influences the definition of cyberspace, which is strongly conditioned by the geostrategic context in which they were born. In turn, as Daniel Kuehl (2000) shows, the environment which is shaping „national security in the information age" is dominated by four critical new developments: 1. the emergence of cyberspace as an operational environment for business, politics , and warfare; 2. the impact of digital convergence, in which essentially any form of information can be expressed digitally and then combined, changed and re-used in ways the originator has no control and little or no awareness of; 3. the growth of global omnilinking; 4. the increasing control of key societal infrastructures by computerized systems.

We observe, therefore, that the attempt to

clarify the connection between cybernetic space, national security, informational era, informational operations confront us with the appearance of a vicious circle, in which each of the elements mentioned above is found in the construction of the significance of the others.

During the Cold War, the combatants had no hesitation in delimiting and enumerating the threats they needed to combat, namely mass destruction weapons, violating air or ground space by the opposing powers, countering the propaganda messages.

With the advent of digital field, the very composition of the threat has changed. In the cybernetic space, it is no longer sufficient for the state to prepare itself and to arm itself with counterattack weapons. The cyber offensive can take place in the home of each of us. We should all be able to defend ourselves against threats coming through the Internet cable. The degree of technological development and of the computerization of a company is strongly correlated with the cyber risks to which it is exposed.

Because the degree of Internet penetration across the globe is not the same, being dependent on population density, average age, per capita income, education level, existing telecommunication structure, etc., neither the benefits or the risks determined by human interconnectivity are not similar. If in North America the internet penetration rate is 89.4%, and in Europe 87.7%, in Africa it is only 39.6% (https://www.internetworldstats.com/stats.htm). Therefore, the destructive effects of an attack will be directly proportional to the level of connection to the world network. However, the numbers are getting closer to 100%, and the growth rate of the spread of the Internet tells us that in a short time this network will truly become a world wide web. Therefore, the cyber war, or the computer war as it was called, becomes with each day a real threat. Ukrainian scientist A. Merezhko (2014) believes that "cyber warfare is the use of the Internet and other information technology tools related to it by a government in order to damage another country's military, economic, political and information security as well as its sovereignty" (Merezhko, 2014).

The US Department of Defense defines cyber warfare as "politically motivated computer hacking aimed at sabotaging and espionage. It is a type of information war that is sometimes considered analogous to traditional armed conflict" (DOD - Cyberspace, 2011). In contrast, the SecurityLab.ru argues that cyber warfare is conducted through Internet in order to put the government computer systems out of order.

We observe that each of the definitions emphasizes the point of view of the issuing entity, emphasizing either on the motivations that animate this type of conflict, either on the environment in which it is carried out, or on the effects that it causes.

CIBERNETIC OPERATIONS

Despite today's ubiquitous cyber operations, found in both the activities of the great powers and the actions of smaller entities, it was not the same until 1991 when the first military operations in the cyber space during the Gulf War were attested. Although they have a huge fighter potential, cyber operations managed to capture the attention of public opinion only after the 2007 attack on Estonia, when the whole country was unable to function, being attacked through banks, ministries and numerous commercial entities.

Hostile actions in the cybernetic environment can be extremely diversified: cyber attacks (against a computer system), cybercrimes (which seeks the acquisition of material benefits through identity theft, deception), cyber espionage, subversion, propaganda, cyber terrorism. Thus hostile actions can include intrusion, surveillance, copying of data, espionage, intellectual property theft, data manipulation, data destruction, control of devices and systems, kinetic effects through device control, destruction of devices and property, destruction of critical infrastructures.

The literature reflects an abundance of information that refers to the danger that China and Russia represents in terms of cyber offensive. It may be areality or a perception bias due to the fact that access to western literature is easier.

Soon cyber attacks confirmed the collective expectation they are a serious problem addressed to national and international security. In 2008, American computers were attacked, through a

single external memory support connected to an army laptop in the Middle East. In this way an undetectable spyware program then infected the classified and unclassified systems and thousands of pages of the Pentagon were taken over by externally controlled servers. To resist to such cyber attacks a new specialised unit was created - USCybercom.

The cyber war took a concrete form during the Russian-Georgian conflict, when the Georgian authorities were electronically restricted the ability to access information and to distribute information to their own citizens and to international public opinion. Georgian banks have tried to protect themselves by suspending online activities. As a result, the attackers simulated attacks against other banks that appeared to have originated in Georgia. Thus, the Georgian banking system was isolated from the international banking system by other countries, and Georgian banking system suffered significant losses that weakened the reactive capacity of the state as a fighting party.

Since then, cyber warfare has become more and more effective. Viruses dedicated to weakening the battlefields of enemy states have appeared. Although not yet verbalized, it may say that the third world war has begun and it is cybernetic. In 2010 the Stuxnet virus was designed for the purpose of taking over the cyber infrastructure of the states. At that time, the context proved itself to be very favorable - the vulnerabilities related to the information systems were numerous and the cyber security culture was a only a desire. Due to the magnitude of the phenomenon, 2010 was considered the year of vulnerability. Banking systems have been attacked by trojans like Zeus or SpyEye, used to steal confidential data from banking systems. The trojan Zeus has become one of the best-selling trojans on the black market due to the ease with which it can be configured to launch a computer attack.

In 2011, Duqu was discovered, a Trojan with similar Stuxnet features, but designed to act as a backdoor to the infected system and steal confidential information.

The following years were notable because of an increasing number of persistent cyber attacks, with a significant impact on national security, of which we can mention Flame3, Wiper, Mahdi, Shamoon, Gauss - malware produced by state actors, used against some critical infrastructures (transport resources energy, banks, government agencies, universities).

According to reports prepared by companies operating in the field of security of information systems, the forecasts are not at all encouraging.

CHINA:

Chinese military doctrine consists in the combination of information technology and information operations, by including SIGINT intelligence, cyber-attacks and operational confrontations in the electromagnetic spectrum (Wortzel, 2014, p.vii). China defines the virtual battle space as being created by technology, computer and web, but subjected to human control and having multiple effects on it (Yufu and Xiaosong,2008). Virtual battle space includes cybernetic space (saibo kongjian), information space (xinsi kongjian), and digital space (shuxue kongjian). The purpose of the Chinese People's Liberation Army (PLA) i is to paralyze or weaken the decision-making capacity of state authorities while affecting the potential for war on the political, economic, military, including civilian housing and community infrastructure (Chang-Ho, 2009).

Therefore, Chinese military strategies have included civilian houses and their supporting infrastructure in the war battlefield. The Chinese People's Liberation Army (PLA) is part of the „integrated network electronic warfare" theory (INEW). Ye Zheng discusses integrated network information attack (wangdian yiti xinxi gongji) as integrating electronic warfare and computer warfare to destroy the enemy's information systems and to preserve one's own (Zheng, apud Wurtzel, 2014). Just as INEW theory seems to have evolved from Chinese research into Soviet military doctrine, the PLA's ideas is a „systems-versus-systems" form of military confrontation in the 21st-century battlefield, dependent on space, cyber, and various information technologies (Wurtzel, 2014).

Thus, the targets of cyber attacks have become energy supply systems, civil aviation systems, industries conditioned by information systems, transport systems, television, telecommunication systems.

Looking back, the idea of war beyond war can be found hundreds of years ago in Machiavelli's work, but it was never as tangible as it is in the era of cyber warfare.

RUSSIA:

The studies carried out by the Russian experts, as it results from the open source literature, are mainly technical, focused on how algorithms can be developed and used in modeling computer systems.

Among the first examples of Russian offensive actions is a robbery that was mediated by cyberspace. Several million dollars were stolen from Citicorp, using a remote computer of a person from St. Petersburg. The model was quickly taken over by organized crime in Russia and used extensively.

The importance that Russia attaches to hostile cyber actions is suggested by the fact that one of its most important analysts, Vitaliy Tsygichko, developed a „coefficient of information security" analysis for the Central Bank of Russia, by which he can estimate the vulnerability of cyber systems to attacks. Cyber weapons are considered capable of destroying the banking system, the telecommunications system, energetic system, to affect the administration, in fact, everything that means life support system. Cyber weapons cause chaos, mistrust and panic in society.

In the process of regaining influence in a geopolitical context in which instability is a permanent feature, the use of all available weapons by the great powers seems to be a common strategic dimension. Usually, the targets chosen of the Russian government are located in Europe, where most of the NATO and EU member countries are located.

Russian literature insists on the psychological impact that the financial markets collapse or the economic system may have. The idea that the economy of the adversary is a viable target for cyber-attacks led by Russia is obvious. Moreover, president Putin himself said that increased access to information through the Internet is „one of the most penetrating components of US expansionism in the post-Soviet sphere of influence" (Nocetti, 2015, 129).

Particular attention is also paid to securing their own computers, the Russian authorities being interested in cyber security products and services. In fact, the founder of Kasperki Labs is Eugene Kasperski, a former KGB officer who created his own hacker team, known as the GREAT - Global Research and Expert Analysis Team. This team offers support to intelligence services in investigations and operations. Cyber attacks as Stuxnet, Flame and Gaus, attributed to the US government, were investigated by Kasperski Labs (Gewirtz, 2012, 9).

After the occupation of Crimea by pro-Russian activists in 2014, the cyber dimension of the war was quiclky on the battlefiled - the Ukrainian web pages were compromised, the access of the Ukrainian users to the Internet services was blocked, the telecommunications were exploited, the mobile phones and wi-fi networks were used for identifying fighters. On 23th of December, 2015, cyber operations included the decoupling of Ukraine's energy supply network, affecting more than 80 000 households in three Ukrainian districts. This attack was the first that targeted the electrical infrastructure of a country (Detsch, 2016, 21-23). It appears that the infection was carried out with the trojan BlackEnergy, implanted with the malware program called KillDisk (Siboni, 2016).

Russia's illegal activities in cyber space have also led to widespread reactions from Western states. In 2018, the US Department of Justice announced the indictment of seven Russian agents who participated in actions against companies and Western states. The authorities in Australia, Canada and New Zealand, as well as the EU and NATO themselves have taken a stand against Russia. The Netherlands has expelled four spies considered guilty of a cyber attack on an international organization based in The Hague. The experts of the Cyberint Center in Romania also draw attention, in turn, that the attacks coming from the Russian space have not only multiplied lately, but have also increased in complexity (https://www.digi24.ro/stiri/externe/ russia / investigation-international-against-Russia-7-agents-defendants-in-US-4-spies-expelled-from-Dutch-1008325).

Russian leaders have also accused that the number of cyber attacks against Russia increased several times and President Putin said that „some countries are trying to use their dominant position in the global information space to meet not just economic goals but also military and political ones", referring to the fact that the United States has benefits from the fact that the servers of the largest social networks used globally were on their territory (Adamczyk, 2014).

In conclusion, it can be seen that Russia has

the entire spectrum of military operations, either to block the activity of one state (Estonia), as a method of fighting among others (Georgia) or as an important dimension of the hybrid war (Ukraine).

CONCLUSIONS

Cyber warfare is an indisputable reality of our day. In this paper I have chosen to present some distinctive elements of the Chinese and Russian strategy, as essential competitors of the European Union.

Despite the official statements that define themselves as victims of cyber operations, Russia and China have defined clear ways of cyber intervention on the enemy / competing states.

Every state is nowdays in the position to allocate considerable human and material resources to enable itself to maintain the security state of the cyber environment.

ACKNOWLEDGMENT

This research was supported by Romanian Ministry of Research, project number 3N/2019.

REFERENCE LIST

*** (2013) Strategia de Securitate Cibernetică a României, p. 7, diponibil la https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accesat la 30.08.2019

***(2003) National Strategy to secure cyber space, available at https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, pVII, accesed at 30.08.2019

Adamczyk, E. Putin: Russia must defend against cyber attacks, UPI News Track, (October), 2014, http://www.upi.com/Top_News/World-News/2014/10/01/Putin-Russia-seeking-cyber-security-not-Internet-kill-switch/9611412184738/

Chang-Ho, W. (2009), Chueh-chi I Tong Ya: Chu-chiao Shin Shihchi Chieh Fang Chun (East Asia Rising: Focus on the People's Liberation Army in the New Century), Taipei, Taiwan: LiveABC Interactive Corp.,

Darczewska, J. (2016) Russia's armed forces on the information war front. Strategic documents, Centre for Eastern Studies, available at https://www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf, accesed 19.09.2019.

Detsch, J. (2016). Did Ukraine Power Grid Hack Give Russia an edge?, Christian Science Monitor 15, 2, 21-23.

Gewirtz, D., (2012). Cyberwar Spotlight: Russia, Journal of Counterterrorism and Homeland Security International, 18, 4, 8-10.

https://www.digi24.ro/stiri/externe/rusia/ancheta-internationala-impotriva-rusiei-7-agenti-inculpati-in-sua-4-spioni-expulzati-din-olanda-1008325

Internet World Stats (2019) World Internet usage and population statistics, available at https://www.internetworldstats.com/stats.htm, acesed 20.09.2019

Kuehl, D. T. (2000) Statement of Dr. Daniel Kuehl, School of Information Warfare & Strategy, National Defense University, For the Joint Economic Committee, February 23, available at https://www.jec.senate.gov/archive/Documents/Hearings/kuehl22300.htm, accesed at 29.08.2019

Kuehl, D.T. (2009). From Cyberspace to Cyberpower: Defining the Problem. În F.D. Kramer, S.H. Starr and L.K. Wentz, Cyber power and National Security, Washington D.C., National Defense University Press, Potomac Books.

Merezhko, A. A. (2014). Draft Convention on prohibition of the use of cyber warfare in the global information and computer network (the Internet). Center for Policy Studies in Ukraine. Available at http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57.

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance, The Royal Institute of International Affairs. London, UK, 2015.

Siboni, G. and Magen, Z. (2016) The Cyber Attack on the Ukrainian Electrical Infrastructure: Another Warning, Institute for National Security Studies Insight, 798.

Thomas, T.L. (2009). The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force, Fort Leavenworth, KS: U.S. Army Foreign Military Studies Office.

Wortzel, L.M. (2014). The Chinese People's Liberation Army And Information Warfare, available at https://publications.armywarcollege.edu/pubs/2263.pdf, accesed 19.09.2019,

Yufu, W. and Xiaosong, Z. (2008). Junshi Xinxi Youshi Lun (Theory of Military Information Superiority). Beijing: National Defense University Press.

Zheng, Y. (2007), Xinxihua Zuozhan Gailun (An Introduction to Informationalized Operations), Beijing, China: Military Science Press.