Scientific Journal of Silesian University of Technology. Series Transport
Zeszyty Naukowe Politechniki Śląskiej. Seria Transport

Volume 106 **2020**

p-ISSN: 0209-3324

e-ISSN: 2450-1549

DOI: https://doi.org/10.20858/sjsutst.2020.106.11

Journal homepage: http://sjsutst.polsl.pl

Article citation information:
Moșoiu, O., Bălăceanu, I., Mihai, E. Cyber terrorism and the effects of the Russian attacks on democratic states in East Europe. *Scientific Journal of Silesian University of Technology. Series Transport*. 2020, **106**, 131-139. ISSN: 0209-3324.
DOI: https://doi.org/10.20858/sjsutst.2020.106.11.

Ovidiu MOȘOIU[1], Ion BĂLĂCEANU[2], Eduard MIHAI[3]

CYBER TERRORISM AND THE EFFECTS OF THE RUSSIAN ATTACKS ON DEMOCRATIC STATES IN EAST EUROPE

Summary. From the analysis of large-scale incidents in the field of cyber terrorism and the possible influence of the Russian government, it was concluded that cyber attacks represent threats to NATO member countries and were included in the list of security threats identified in the NATO`s New Strategic Concept of 2010. This conclusion makes terrorism a new dimension, a cybernetic one, as an adaption of terrorism to the new era and a new defence field to be taken in consideration – the cybernetic field. For these reasons, in 2016, NATO recognised the importance of introducing virtual space as an operational domain, which opened the gates to cyber security, and invited member countries to contribute to the development of cyber defence projects. The solution of the cyber attacks has created the conditions for normal functioning of any state critical infrastructure.

Keywords: cyber terrorism, terrorist organisations, cyber threats, cyber space, internet services, cyber warfare, computer networks, virtual space

[1] "Henri Coandă" Air Force Academy, Brașov, Romania. Email: ovidiu_mosoiu@yahoo.com
[2] "Carol I" National Defence University, Bucharest, Romania. Email: balaceanugion@yahoo.com
[3] "Henri Coandă" Air Force Academy, Brașov, Romania. Email: mishued2004@gmail.com

1. INTRODUCTION

The security actions for cyber space represent a common effort of those who apply law, governments, technological industries and individuals in society. In order to secure the cyber space, a great understanding of the phenomenon of cybernetic terrorism is needed, a contemporary phenomenon that has the cyber space as a battlefield and is proliferated through the internet, without referring to physical destruction of the network, but the establishment of terror among the state and the non-state actors who use it. Thus, the term cyber-terrorism refers to the use of tactics and techniques of informational warfare by the terrorist organisations, which affect the cyber space. Moreover, cyber terrorism operates exclusively in virtual space and does not physically destroy the infrastructure that supports the existence of the cyber space. While computer-based terrorists seek an impact on the concerns and actions of "real" people from the "real" world, they operate within the virtual world of cyber space to manipulate these actors.

In 2000, Dorothy Denning, an information security researcher in cyber terrorism, define cyber terrorism as "a *convergence of terrorism and cyber space. Cyber terrorism consists in planning illegal attacks and threats against computers, networks and stored information on them, in order to create a fear climate or to exert pressures on a government, a non-governmental international organisation or through population to fulfil certain objectives related to pursuit of a political cause, religious, racial or ideological, by affecting the integrity and confidentiality of information, computer system and computer networks"* [3]. Later on, the fast development of cyber terrorism required new global strategies, with responsibility for ensuring cyber security to all the actors involved in fighting against the cybercrime phenomenon. As can be seen, cyber terrorism does not differ from conventional terrorism as a goal, it is taken seriously by the government and it is intended to secure the operating means, the networks and interconnected critical infrastructure [8].

From the military point of view, the cyber space has determined the appearance of cyber weapons, used in new types of military operations, which differ from the classical ones by the way of manifestation, the aim being the same – eliminating the opponent. Whatever the type of conflict will be in the future, cyber terrorism will be integrated into all forms of war (conventional or unconventional). Due to the cross-border features of government-led internet actions, organisations as NATO and the EU have recognised the importance of the cyber space and launched a series of cooperation projects between member states on cyber security, training and education in this multidisciplinary field.

In 2014, Laurian Gherman, highlighted the importance of the cyberspace domain "*if our ability to acquire and to send information is reduced by the enemy, our concept of information superiority is doomed. From this point of view, today and in the future, the electronic warfare role will be very important. For this reason, the physical domain of the electromagnetic spectrum should be at the same level as the land, maritime, air and space domains and all should be networked*" [5].

The appearance of the Russian hybrid war in the Ukrainian area did not end with the annexation of the Crimean Peninsula (2014). The success of this operation was accomplished through the use of elite troops (the so-called "green-men") along with an informational warfare campaign conducted by various Russian proxies. Moreover, there are reasonable suspicions of using the electoral war, generated by the Russian Federation`s involvement in the US presidential campaign (2016), the elections in Germany (2015), France, Netherland and Ukraine (2019), and to organise a plot to overthrow the pro-NATO government in Montenegro (2016). All these analysed aspects allow us to conclude that an electoral war is

happening, orchestrated by the Russian Federation, and is taking place at this time, with difficulties in imagining the implications, both in the political and the economic spheres.

The lesson learned, especially from the three cases of cyber attacks (over Estonia, Georgia and Ukraine), have shown different faces of the security and the cyber defence from a technical, diplomatic, sociological and military view. As a result, the cyber security measures to be taken must be the result of a union of forces between government IT specialists, the private and public departments, as well as state actors specialised in cyber security of economic structures.

2. THE CYBER ATTACK OVER ESTONIA

The first massive cyber attack in Eastern Europe was recorded in Estonia, one of the Baltic republics that were embedded in the Soviet Union in 1940. After the dissolution of the Soviet Union, Estonia regained its independence and quickly began the process of economic, political, social and military reforms. It joined the EU and NATO in order to secure its national security. The Estonian authorities saw Russia as the most serious threat, and integration with Western structures was the solution to overcome this threat. One of the main disputes in bilateral relations was "the issue of the Russian minority in Estonia that represents 26% of the population" [7].

Since April 2007, tensions between Estonia and Russia increased significantly as a result of the Tallinn (Estonian capital) authorities' decision to move the Soviet Monument to the centre of the city (the monument commemorates the Soviet soldiers who liberated Estonia). After the statue was moved, the relationship between Estonia and Russia became tense, with the Kremlin "*accusing the Tallinn authorities of violating human rights, for which they demanded the resignation of the Estonian Prime Minister*" [9]. At the same time, violent fights broke out in the streets between the police and the Russian minority in Estonia, protests in front of the Moscow Embassy in Moscow and massive cyber attacks. The attacks flowed as follows: in the first phase, their coordination was done through forums and the synchronization of human actions, and in the second phase coordination was delegated to the command and control servers of the botnet network. The second phase ran from April 30th to May 18th and ran in *four waves* of varying intensity, focusing on different targets and using various attack techniques. *The first wave* of attacks on May 4th consisted of DDoS (Distributed Denial of Services) attacks on DNS sites and systems. *The second wave* considered the peak of the attack, took place on May 9th; then the number of hostile acts began to decline. On May 11th, paid botnets ended DDoS attacks with government and financial services sites inclusive. *The third wave* of attacks began on May 15th and included DDoS botnet attacks against government and financial industry websites. *The fourth wave* of attacks again consisted of attacks on government sites and banks. The DDoS attacks successfully targeted the websites of all ministries, two large banks and several political parties. Hackers "*have been able to close the parliament's e-mail server and have disabled ATMs*" [9]. One of the Estonian banks that was the victim of cyber attacks estimated losses of around $ 1 million. However, when assessing losses at the end of the attacks, it was surprisingly found that the damage done by cyber attacks was relatively low.

Unlike the first phase attacks, the second phase was based on the botnet, which is today considered the main vehicle and platform for cybercrime. Cybernetic (cyber attack) in Estonia since 2007 has been widely debated in the media and has been called "*the first cyber war in history. This has shown how new technology could be used to attack a modern country. It has*

been proven that the attacks came from Russia, with most DDoS attacks being initiated from Russian IP addresses"[11]. A lot of attackers used computers in Estonia, which indicated the Russian minority. Even though the technical experts from the European Commission and NATO found no evidence that the attacks were committed by the Russian authorities, they were considered to come from the Kremlin. A member of the Russian youth organisation, NASHI, affiliated with the party of Vladimir Putin, confessed that "*he stood behind the attacks*" [6].

The supposed objectives of the cyber attacks were to try to influence the Tallinn authorities to withdraw the decision to remove the monument. Another objective was to test the Russian capabilities of cyber war and to see NATO's reaction when one of its members was attacked in a new field. In addition, a third objective was linked to the fact that the Estonian society is dependent on the Internet. Cyber attacks have been carried out to prove that NATO and the EU would not defend the Estonian society from the Russian attack and the Russians do not need tanks to cause damage to Estonia. Due to these attacks, Russia's political objectives were not achieved as the monument was not moved, and Estonia became a leader in cyber security. NATO has accelerated its cyber defence projects and created the Centre for Excellence for Cooperation in Cyber Defence, located near Tallinn. Estonia and Western allies have secured mutual support for future large-scale attacks on IT and C infrastructures, thus increasing the potential risks and costs for an opponent who tolerates or even uses volunteer groups to attack foreign Internet infrastructure. As a result, Estonia has become closer than ever to Western security institutions, while Russia's cultural and political influence on Estonia has diminished. Regardless of the fact that Russia's foreign policy circles were defined as strategic objectives, cyber attacks against Estonia have not advanced political causes on the part of Russia.

The first lesson learned by the Estonians, as well as the world over, was that cyber security and defence of the national network involved not only technical details of the attacks but also strategies and policies of a technological nature. CERT-EE team tactics have been to maintain critical online sites, such as banking sites, rather than government websites, even if their failure was a sign of weakness on the part of the country's government, and was a real success for attackers. Another tactic was to keep the parliament's email server even in the network, even if it was necessary to physically move the server from one internet provider to another. This has hardened the attackers, who have put all their attention and energy in shutting down this server without having to worry about other critical targets.

In conclusion, action efficiency is a basic feature of cyber attacks. In the case of Estonia, the aggressors did not achieve their political goals. The main tool of all the attacks was the brutal DDoS attack, which took place primarily with massive botnet networks and later, by patriotic hackers using previously prepared tools. In Estonia, government sites, as well as banks and newspapers online, were disrupted. As a result of the hostile action, most internet services collapsed and their restoration was rather cumbersome. However, the Estonian information society seemed to be quite resilient, which made it unstoppable after the cyber attacks.

3. CYBER ATTACK OVER GEORGIA

The second cyber attack took place in Georgia and was called "*the first war in the air, at sea, on the ground and in cyberspace*". Georgia regained its independence after the collapse of the Soviet Union, having a long history and strong national consciousness; it was different from

the other Soviet countries. Since the early 1990s, Georgia has wanted integration with the West. This trend has been strengthened since 2003 when the Rose Revolution took place, and President Eduard Shevardnadze was overthrown. The newly elected president, Mikhail Saakashvili, engaged in integration with Western structures and attempted to re-integrate Georgia's radical provinces – South Ossetia and Abkhazia. His attempts received a strong reaction from Russia and led to the outbreak of the 2008 war. This conflict, which began on August 7th and lasted for 5 days, was a reminder of classical states versus states in conflict, which seems to have been forgotten in the 21st century. Despite the fact that the war was classical, and the army's behaviour on the battlefield recalls the 20th century, a certain aspect of it was a novelty - it was the first war that took place in the air, on the ground, at sea and in cyberspace.

The first informational attacks occurred several months before the outbreak of the war. On July 19th, the security firm "*FireEye informed about DDoS attacks against Georgian sites*" [4]. A scenario similar to previous attacks was repeated on a larger scale on August 8th and coincided with the entry of Russian troops into South Ossetia. The attack by Russian hackers can be divided into two phases. *In the first phase*, they focused mainly on Georgian news and government websites. *In the second phase*, a lot of patriotic hackers joined the campaign against Georgia. Until August 10th, most Georgian government sites were inoperative, and the Georgian government could not communicate with the rest of the world via the Internet. The content of the Georgian President's website was replaced by images that described M. Saakashvili as Hitler. Also, banks did not work in Georgia, as did mobile phones. According to Captain Paulo Shakarian's views in the US Army, "*Russian hackers have tested their skills and ability to lead limited attacks*" [10].

There were two other interesting aspects of Georgia's cyber attack. The first is about coordinating conventional blows with cyber attacks, which are often unseen. However, there are two examples that could indicate the cooperation between classical and cyber forces. The first example was that conventional attacks have omitted media and communications sites, leaving these targets for cyber attacks. The second example was an attack on diesel generator rental sites that wanted to support the conventional blow to Georgia's electricity infrastructure. The second aspect interestingly includes training IT tools, training, creating special sites to do these attacks, which may indicate that Russia has been preparing this war for a long time. Access to available Russian tools and instructions for use cannot be prepared in one day. Following a massive disruption of sites, the Georgian authorities first tried to filter IP addresses from Russia, but they quickly changed tactics and used non-Russian servers. Later, the Georgian authorities requested help from the United States, Poland and Estonia, and Georgian servers were relocated.

Georgia's cyber attack was a manifestation of an informational or media war intended to disrupt its access to any news source. The authors pursued *three main objectives*. *The first* was to show the whole world the fragility of the Saakashvili regime, which lost control of its own state, and the paralysis of the state following the Russian invasion. *The second*, addressed to the Georgian society, was to interrupt any source of information and to present its own propaganda in order to spread chaos and misinformation to undermine the morale and faith of the population in the government. *The third* objective is linked to the second phase of attacks against the economic system. Most likely, it wanted to cause serious damage to Georgia's economic development and persuade the population to withdraw support from Saakashvili. The objectives were not mainly achieved due to US and EU aid (CERT, CERT-EE, CERT-PL, CERT-FR). Government sites were restored, and the Georgian society

regained access to information. The US also pledged financial support to the Georgian government.

The lesson learned in this context, by creating a change of mentality, globally, such as that cyber security is accomplished by technical means, but it is people, strategy, commitment, and not computers, which are simple tools, weapons of attack. Participants in DDoS attacks were motivated by factors such as adherence to group rules, social validation and contagion, which contributed to the success of the attacks. The rapid influence of the population by online means was a good example of copying and using, for the Russian authorities, which was seen a year later in Georgia's cyber attack that accompanied the conventional war. In this case, a new element - online propaganda appeared. Georgia was perfectly aware of its economic, military, and political inferiority to Russia and, through public relations services, Aspect Consulting, a media propaganda used as a weapon against the Russians. International media agencies and special Western media were bombarded with information that Georgian civilians were being attacked by the Russian army, and media relations yielded favourable evidence to Georgia and unfavourable Russia. After tensions were doused, Western newspapers that held Georgia's position and accused Russia became more critical on the circumstances in which the conflict started, having realised the false theory that Georgia was the innocent victim of Russian aggression.

In conclusion, the lesson learned from the military and legislative point of view was that the meaning of an effective response to cyber attacks of the size and type of Georgia is limited by legislation. More importantly, they include promoting effective international technology cooperation, as there is no way for a country to coordinate its defence against attacks from other jurisdictions. However, it must be taken in consideration that no national or international entity has the authority to legislate in the cybernetic field, national efforts will need to work with international instruments of different fields and with a different focus. In addition to that, the attack technique was interesting. There were similarities that may indicate that the aggressor could be the same as in Estonia. Although, the case of Georgia seems a little bit different, in a way the attack was more sophisticated. Government sites, as well as banks and newspapers online, were disrupted. As a result of the hostile actions, most internet services collapsed and their restoration was rather difficult.

4. CYBER ATTACK OVER UKRAINE

The third cyber attack, massively recorded in history, was the one of Ukraine, which has been considered as a case of cyber spying. Prior to the 2014 revolution, Ukraine experienced a rather typical series of cyber incidents, of which the most common were botnets controlled by DDoS. Often, they came as retaliation for unpopular government initiatives (for example, when the authorities tried to close the file-sharing site, http://www.ex.ua). By the end of 2012, part of the public's frustration was channelled into the deterioration of politically motivated (“graffiti digital”) sites in the Ukrainian government's virtual space. In 2013, a serious malware class was discovered, and network vandalism sparked an increase in cyber spying, for which cyber security companies developed a list of names: RedOctober, MiniDuke, NetTraveler and more. After the revolution began, in February 2014, ordinary Ukrainians became acquainted with the combination of hacking and political activism (“hacktivism”), in which attackers carried psychological warfare through the Internet. Although a large number of people have been exhausted by major political events that have shaken Ukraine, it has been hard to ignore the publication of leaks of Ukrainian government documents. The most

prominent hacking group was CyberBerkut, whose famous attack created serious problems *for the country's infrastructure*.

There have been significant cyber-spying operations directed against victims of Russia's strategic interests, particularly with regard to the situation in Ukraine. However, there were no profound, coercive and harmful attacks similar to those taking place in Estonia in 2007 or in Georgia in 2008. Examples reported by the NCA in Ukraine include mainly Denial of Service (DoS) and Distributed Denial of Service (DDoS), designed to undermine the Ukrainian telecommunication infrastructure. For attackers, these were low-risk ways to disrupt the flow of information from the Ukrainian national security space, as well as a way of selectively and temporarily silencing the online voice [7].

In the Russia-Ukraine conflict, the operations in informational networks were not limited to the notion of cyberwar. An examination of the sustained tensions suggests that this was warfare for strategic theft and manipulation of information, not the widespread application of destructive cyber attacks. Cyber espionage campaigns in Russia over time and against numerous targets undoubtedly have a considerable advantage in understanding, anticipating and, in some cases, overcoming enemies. This approach may have made DDoS and other destructive attacks less necessary or preferable. One of the most important aspects of the three cases is their author. The cyberspace architecture does not allow us to unequivocally assert who was responsible for cyber attacks. The fact is that most of the attacks came from Russia, and this can lead to *three hypotheses*. [1]

The first hypothesis is based on the assumption that the attacks were carried out by Russian amateurs, patriotic hackers who wanted to cyber-attack to express their affront to the offence brought about by the politics of Estonia and Georgia. This assumption is unlikely, mainly due to the lack of technical skills of these hackers. During the attacks, advanced botnets consisted of using thousands of computers that are inaccessible to average Internet users. In addition, for Ukraine, the Russian social networks of hackers were not involved. *The second assumption* was that Russian cybercrime groups on their own, especially Russian business networks, carried out the attacks. The use of advanced botnets owned by Russian cybercriminals has highlighted the commitment of Russian hackers. These groups are mainly seeking money. It is hard to mention the financial potential benefits that could have been obtained by attacking Georgian, Estonian and Ukrainian sites. Because of this, these assumptions seem improbable. *The third theory* is based on the presumption that the Russian authorities have committed cybercriminals from the Russian Business Network to lead attacks against Estonia, Georgia and Ukraine. This sentence seems most likely from several considerations. Russia wanted to punish these countries, but it was unable, especially in the case of Estonia - a NATO member - to hire the state to sponsor the offensive. So it was convenient to hire cybercriminals who carried the offensive campaign on behalf of the Russian authorities. The second important aspect is the full control of the Russian Internet streams by the Moscow authorities, so an attack of this magnitude could not have gone unnoticed by the authorities, thus they were made with the tacit agreement of the government Russian.

The lesson learned in Ukraine was the fundamental lack of understanding of cyber security on the part of users. Therefore, each institution attempted to develop a malware "literacy campaign" to let employees know how to start system infections and how attackers can control their computers then to steal documents, all through a small program, unauthorised dimensions that can be hard to detect. Lack of experience and perception of the cyber-threat (from both the public, population and private institutions) is the key to making international consensus on cyber security issues more time-consuming. On the other hand *"the majority of the world's states invest billions of dollars in online attacks that regard*

information in all areas (politics, diplomacy, economy, defence, culture, science, and so on)" [2].

5. CONCLUSIONS:

Following the analysis of the three cases of cyber attack, we can state that there is a trend in the future of military competition in cyberspace. From a military point of view, the information society has led to the development of specific cases of attack in the new competitive space – the cyberspace. Similar to classical actions, both simple tools and actions are used, as well as cyber attacks carried out according to hybrid rules and laws. In the case of malware in the system, the problem of IT specialists has gone beyond the boundaries of IT and C and has become a cyber security issue, which can be a major challenge with repercussions on the security of *critical state infrastructures.* Viruses can also be a military tool with destructive effects on information.

Based on the military and legal lessons learned from the recent public cyber attacks, it seems that a contemporary way to cyber-attack a country is "*using the grey area"* in the law that does not invoke the Law of the organisation of the armed conflict (LOAC), as the International Humanitarian Law. The authors of the attacks act in particular in an area that triggered the application of relevant provisions in criminal law, poorly developed in many countries, and which has unsolicited ground for cross-border cooperation. This will require time to reach an additional consensus on international legal issues of cyber defence. So far, only 23 countries have ratified the crime of cybercrime and only a few have been able to genuinely test national defence for the law. Moreover, the training of countries in the field of cyber security is different and is related to their degree of economic and military development.

The cyber operational environment will continue to evolve, presenting to the military forces various challenges in the form of threats posed by opponents, which carry out actions ranging from conventional to unconventional, with capabilities that include state-of-the-art weaponry and technology. These opponents can include extremely well-trained and highly-equipped conventional forces as well as specialised forces to conduct irregular fighting, resulting in a force that uses the hybrid threat.

References

1. Bălăceanu Ion, Virgil Manea, Ovidiu Moșoiu. 2019. *Sistemul interinstituțional de prevenire și combatere a amenințărilor neconvenționale în zona de interes strategic a României*, "Henri Coandă" Brașov: Air Force Academy Printed House. ISBN 978-606-8356-68-6. [In Romanian: *Interinstitutional system for preventing and fighting unconventional threats in the area of strategic interest of Romania*].
2. Cioacă Cătălin. 2009. "Cyber – Terrorism, an Instability Global Source". *Review of the Air Force Academy* 2(15). Brașov: "Henri Coandă" Air Force Academy Printed House. ISSN 1842-9238.
3. Denning Dorothy. "Cyberterrorism". Available at: http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.

4. Foxall Andrew. 2016. “Putin’s Cyberwar: Russia’s Statecraft in the Fifth Domain”. *Russia Studies Centre Policy Paper* 9. The Henry Jackson Society. Available at: http://www.stratcomcoe.org/do wnload/file/fid/5212.
5. Gherman Laurian. 2014. „Electronic warfare in information age”. *Review of Air Force Academy* 3. Brașov: “Henri Coandă” Air Force Academy Printed House. ISSN 1842-9238.
6. Greenberg Andy. “The State of Cyber Security When Cyber Terrorism Becomes State Censorship”. Forbes.com. Available at: http://www.forbes.com/2008/05/14/cyberattacks-terrorism-estonia-tech-security08-cx_ag_0514attacks. html.
7. Kozłowski Andrzej. 2014. “Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan”. *European Scientific Journal (ESJ)* 3. Available at: http://www.eujournal.org/index.php/esj/article/view/2941.
8. Moldovan Marius, Ion Bălăceanu. 2018. *Reconfigurarea balanței de putere militară în zona estică de interes strategic a României*, București: National Defence University “Carol I” Printed House. [In Romanian: *Reconfigure the military power balance in the eastern area of strategic interest of Romania*].
9. Nazario Jose. *Politically Motivated Denial of Service Attacks.* NATO CCDCOE. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/12_NAZARIO%20Politically%20Motivated%20 DDoS.pdf.
10. *Rețea cu un număr mare de calculatoare virusate ce sunt manipulate de infractorii cibernetici de la distanță, în scopul atacurilor DDoS sau SPAM*. Available at: https://usa.kaspersky.com/resource-center/threats/botnet-attacks. [In Romanian: *Network with a large number of viruses that are handled by remote cybercriminals for DDoS or SPAM attacks*].
11. William C. Ashmore. “Impact of Alleged Ryssuan Cyber Attaks”. SAMS 2009. Available at: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-027.pdf.

Received 19.10.2019; accepted in revised form 20.12.2019