Social Transformations in Contemporary Society, 2018 (6)
ISSN 2345-0126 (online)

CYBERATTACKS AS "ARMED ATTACKS" ON THE OBJECTS OF CRITICAL INFRASTRUCTURE IN LIGHT ARTICLE 5 OF NATO TREATY

Sergii Karasov

Mykolas Romeris University, Lithuania
sergiikarasov@gmail.com

Abstract

In recent years, cyber security has become one of the most actively discussed topics of international law, not only because domestic and inter-State cyber security incidents have grown in number and severity, but also because of the realisation that the technical peculiarities of cyberspace create new and unique legal problems that previously have not been encountered.[1]

In the Wales Summit Declaration on 5 September 2014, NATO recognized that international law, including international humanitarian law and the United Nations Charter (UN Charter), applies in cyberspace. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council (NAC) on a case-by-case basis.[2]

Collective self-defense expressed in Article 5 of NATO Treaty is a well-known fundamental principle of NATO: *"…an armed attack against one or more of them in Europe or North America shall be considered an attack against them all (…)".*[3]

Although Article 5 of the NATO Treaty has no concept of the objects of armed attacks, cyberattacks as "Armed Attacks" can be carried out on Critical Infrastrucutre (CI), and on Critical Information Infrastructure (CII). Such objects can function for both military and civilian purposes. CI for civil purposes can be both in state and private ownership. The types of activities of such objects are important for the exercise of state functions.

Purpose - The present article aims at analyzing concept, types, functions of critical infrastructure and cases of cyberattacks on such objects and to determine the relationship with definition of Armed Attack in light Article 5 of the NATO Treaty.

Design/methodology/approach – the author of the article is comparing legal definitions of CI in-laws of member states of NATO that connects to cyberattacks and come across with differences and common points. The case of Estonia (cyberattack on government networks), Ukraine (cyberattack on CEI) and *Stuxnet* (cyberattacks against CI) are shortly reviewed.

Finding - when it comes to cyberattacks, in most cases, it is conducted on a CII, which is directly connected and is the source of automatic control of critical infrastructure. To date, the most successful such definition is in the strategy for cybersecurity of Lithuania as a NATO member, and a partner of NATO, Finland. Case in Ukraine showed that CI works in disconnected access to the Internet network. However, working personnel periodically violated

---

[1] Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013), 621

[2] Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en

[3] The North Atlantic Treaty, Washington D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

the rules of automated control and connected the Supervisory Control and Data Acquisition (SCADA)[1] to the Internet.

Research limitations/implications – the author uses NATO Treaty, legislation of the member countries of NATO to compare it and three cases of cyberattacks on CI.

Practical implications – the article could be considered by NATO' headquarters (NATO HQ), North Atlantic Council (NAC), Allied Command Transformation (ACT), NATO Communications and Information Agency (NCI Agency), NATO accredited Centres of Excellence, in particularly NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), military legal advisers to the command of NATO allies and partner countries.

Originality/Value – the problem of application of Article 5 of NATO Treaty to cyberattacks is quite new for NATO and partner countries as well. That also causes a novelty of that article – finding that cyberattacks on CI could be invoked right on the collective self-defense for NATO.

Keywords – Cyberattack, Armed Attack, NATO, Critical Infrastructure, Critical Information Infrastructure, Collective Self-Defense

Research type – research paper

Introduction

To date, cyberattacks pose a serious threat to NATO's defense and security. Every time, cyberattacks become more sophisticated to identify and attribute to the attacker. There is no doubt that cyberattacks can create serious devastating consequences for CI of states. This can lead to disastrous consequences.

It is possible that cyberattacks can be committed on CI designed for military purposes. The protection of such types of CI from cyberattacks is very important for the performance of the functions of state defense. In addition, cyberattacks can be used in combination with kinetic attacks, which can cause unpredictable consequences.

Several states have in fact been the object of cyberattacks of which other states were suspected. In 2007, a three-week Distributed Denial of Service (DDoS) attack targeted Estonia.[2] Cyber operations also hit, among others, Azerbaijan, Kyrgyzstan, Lithuania, Montenegro, South Korea, Switzerland, Taiwan, the United Kingdom, and the United States. In September 2010, a computer worm, dubbed Stuxnet, had attacked Iran's industrial infrastructure.[3] In December 2015, Ukraine faced a major escalation in the seriousness of cyberattacks on Critical Energy Infrastructure (CEI).[1]

---

[1] Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control features in the industrial sector and energy transit infrastructure. The security of the SCADA system consists of four major elements: real-time monitoring, detection of anomalies, impact analysis and mitigation strategies.
Limba T.; Plėta T.; Agafonov K.; Damkus M. 2017. Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues 4(4), 561. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

[2] "Cited from: For the facts of the case, see Eneken Tikk, Kadri Kaska, and Liis Vihul, International Cyber Incidents. Legal Considerations (CCDCOE, 2010), pp 18 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 4.

[3] "Cited from: For a comprehensive technical analysis of Stuxnet, see Symantec's Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, version 1.4, February 2011, <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet

ISSN 2345-0126 (online)

Taking into account that the cyber threats and attacks are becoming more common, sophisticated and damaging, it is very important that such actions are countered with a strong commitment to existing international law and the values that it represents. The right to collective self-defense in the case of cyberattacks on CI becomes relevant and necessary for research in international law.

One way of exercising collective self-defence is through a military alliance established to that purpose. The most significant collective self-defence international organization today is North Atlantic Treaty Organization (NATO) as source of stability in world and the transatlantic framework for strong collective defense.[2]

Bearing in mind that NATO has affirmed the applicability of international law and article 5 of the NATO treaty in the case of cyberattacks, there is a scientific need to examine CI within the concept of cyberattack as "Armed Attack" according to Article 5 of NATO Treaty.

The article will focus on analyzing: 1) the concept, types and functions of CI as objects of cyberattacks, 2) cyberattacks against CI: Estonia, *Stuxnet* and Ukraine cases study 3) the consequences of cyberattacks against CI in the light of the right to collective self-defense.

Concepts, types and functions of CI as the objects of the cyberattack

The cyberattacks can be directed at both CI and CII. In modern international law, there is no definition of these two concepts. However, NATO countries and partner countries refer to the Critical Infrastructures Protection Act of the United States of 2001.[3] This is defined CI as system and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[4]

Although governments administer only a minority of the Nation`s CI computer systems, governments at all levels perform essential services that rely on each of the critical infrastructure sectors. Such sectors related to agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping.[5]

In turn, when it comes to cyberattacks, in most cases it is conducted on a CII, which is directly connected and is the source of automatic control of critical

---

_dossier.pdf. Iran claims that its uranium enrichment programme is for purely civilian purposes. Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 6.

[1] "The first case of a successful cyberattack on energy objects has been registered in Ukraine" Ukrainian National News, http://www.unn.com.ua/uk/news/1552689-minenergovugillya-pershiy-u-sviti-vipadok-vdaloyi-kiberataki-na-obyekti-energetiki-zareyestrovano-v-ukrayini

[2] The North Atlantic Treaty, Washington D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[3] Critical Infrastructures Protection Act of 2001, the United States, https://www.govtrack.us/congress/bills/107/s1407/text

[4] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn , Estonia, https://ccdcoe.org/cyber-definitions.html

[5] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn , Estonia, https://ccdcoe.org/cyber-definitions.html

infrastructure. To date, the most successful such definition is in the strategy for cybersecurity of Lithuania as a NATO member,[1] and a partner of NATO, Finland[2].

According to approval of the program for the development of electronic information security (cyber-security) of Lithuania for 2011-2019, CII shall mean an electronic communications network, information system or a group of information systems (included all hardware and software that process, store, and communicate information, or any combination of all of these elements, computer systems; control systems (e.g. SCADA). In addition, it is included networks, such as the Internet; and cyber services (e.g., managed security services). are part of cyber infrastructure where an incident that occurs causes or may cause grave damage to national security, national economy or social well-being. [3]

In Finland's Cyber Security Strategy from 2010, CII refers to the structures and functions behind the information systems of the vital functions of society which electronically transmit, transfer, receive, store or otherwise process information (data).[4]

In a traditional armed attack, the fact that the target is military or civilian would not make any difference: the state where the target is located would be entitled to self-defense because its territorial integrity has been violated.[5]

Hence, Dinstein correctly points out that, if a conventional armed attack against a civilian facility on the territory of the target state would amount to an armed attack even if no member of the armed forces is injured or military property damaged, there is no reason to come to a different conclusion with regard to cyberattacks against civilian systems.[6]

Most CI are not owned by the government, but by the private sector: the governmental or private character of the infrastructure targeted, however, is also not relevant to the determination of the existence of an armed attack against the state. It is not relevant that the computer system is run by a company possessing the nationality of a third state or that the computer system operated by the victim state is located outside its borders (for instance, in a military base abroad).[7]

For a clear understanding of the enemy's real target as CI, the author suggests several examples of cyberattacks on CEI, like some situations during crisis (military) stage, which were used during Tabletop Exercise Coherent Resilience (CORE) 2017 in Ukraine: 1) As a result of cyberattacks, three regions have had their power interrupted. A 750 kV high-voltage substation is disconnected from the United Energy

[1] "National cyber security strategy of Lithuania, Programme for the Development of Electronic Information Security for 2011–2019 (2011)", https://ccdcoe.org/cyber-security-strategy-documents.html
[2] "National cyber security strategy Finland's Cyber Security Strategy (2013)", https://ccdcoe.org/cyber-security-strategy-documents.html
[3] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn , Estonia, https://ccdcoe.org/cyber-definitions.html
[4] NATO Cooperative Cyber Defence Centre of Excellence, Tallinn , Estonia, https://ccdcoe.org/cyber-definitions.html
[5] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 76.
[6] "Cited from: Dinstein, 'Computer Network Attacks', p 106.", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 76.
[7] Cited from: Dinstein, 'Computer Network Attacks', p 106-7.", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 76.

ISSN 2345-0126 (online)

System (UES) of Kray; 2) As a result of a cyber-attack on the SCADA system of telemechanical control, the system lost the opportunity to receive information.[1]

These examples show that CI is the target of the attacker. Situations were used in real practice. A feature of these examples is that such an infrastructure works in disconnected access to the Internet network. However, working personnel periodically violated the rules of automated control and connected the system SCADA to the Internet.

Taking into account the experience of previous cyberattacks on state critical CI facilities, as well as the results of Tabletop Exercise Coherent Resilience (CORE) 2017 in Ukraine, the author suggests the following structure of the objects of cyberattacks in the light of Article 5 of the NATO treaty (Figure 1).

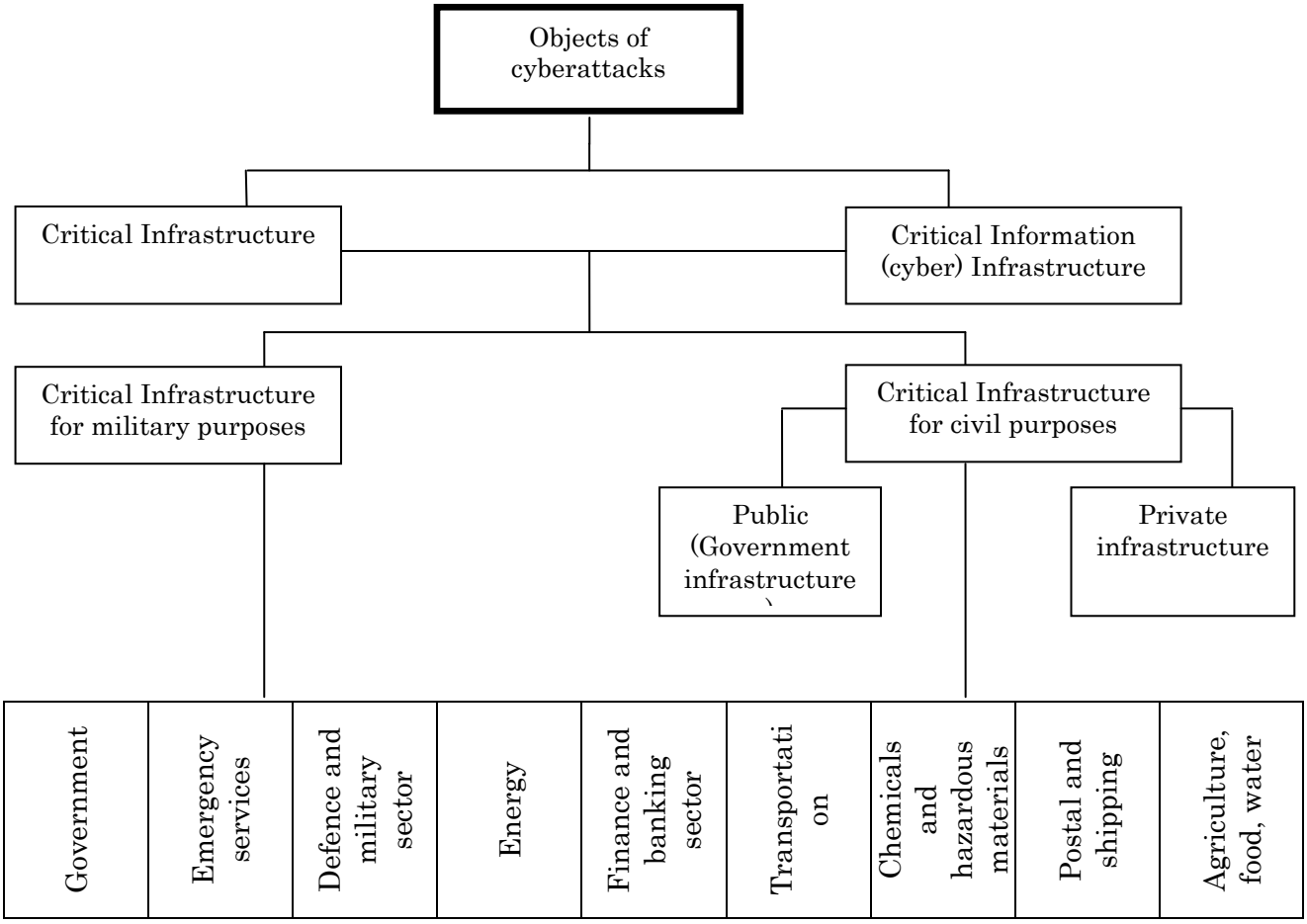

Figure 1. Objects of cyberattacks as "Armed Attack" in light Article 5 of NATO Treaty

From this figure it can be concluded that cyberattacks as Armed Attacks can be carried out on CI, and on CII. Such objects can function for both military and civilian purposes. CI for civil purposes can be both in state and private ownership. The types of activities of such objects are important for the exercise of state functions.

[1] Final Evaluation Report, Advanced Training Course on Critical Energy Infrastructure Security with Tabletop Exercise Coherent Resilience (CORE) 2017, NPS EAG, Kyiv, Ukraine.

ISSN 2345-0126 (online)

Cyberattacks against CI: Estonia, *Stuxnet* and Ukraine cases study

History knows several examples when cyberattacks were conducted on CI. Among them, the author would like to note Estonia (2007), Stuxnet (2010) and Ukraine (2015, 2016) cases. These cases are of an international nature, because, as a rule, cyberattacks were conducted outside the state.

On April 26 and 27 of 2007, Estonia witnessed two nights of unprecedented street riots in the centre of Tallinn, its capital, by youth groups mostly of ethnic Russian origin. The riots had broken out in response to the government decision to remove a Soviet-era Second World War (WWII) memorial, a decision which had been accompanied by intense vocal opposition by Estonia and Russia.[1]

Cyberattacks started in parallel to rioting on streets in the late hours of Friday, April 27, when web pages of Estonian government institutions and news portals came under a wave of cyberattacks.[2] Attacks continued from April 27 to May 18 (3 weeks).

The prime targets (and also those that experienced major effect) were information distribution channels of both the government and the private sector, and business sector websites, specifically, the banks. The work of vital databases, systems or registers of the public and private sector was not disrupted, but there were attacks directed at the national Internet infrastructure. Also, the common emergency number 112 was targeted so that calls were briefly blocked.[3]

The targets for cyberattack were mainly fourfold: servers of institutions that are responsible for the Estonian Internet infrastructure; governmental and political targets; services provided by the private sector; personal and random targets. Notably, traditional CI objects, such as information systems supporting transportation and energy systems, were not targeted.[4]

The cyber effects had both a direct economic and a wider societal effect. As many sectors of commerce and industry rely on ICT infrastructure and electronic communication channels in their daily conduct of business, the overload of e-mail servers, network devices and web servers of internet service providers not only affected large entities such as banks, media corporations, and governmental institutions, but also small and medium-sized enterprises whose daily business activities were seriously impaired.[5] The attacks also affected the nation's information flow to the outside world.

The question of invoking article 5 of NATO Treaty was never seriously considered. As expressed by Mr. Jaak Aaviksoo, Estonian defence ex-minister, it was clear that "At present, NATO does not define cyberattacks as a clear military action.

---

[1] Among others, the foreign minister of the Russian Socor, Vladimir. 'Moscow stung by Estonian ban on totalitarianism's symbols'. Eurasia Daily Monitor, The Jamestown Foundation, 26 Jan 2007. Available at http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=32427

[2] Tikk, Kaska, Vihul, International Cyber Incidents. Legal Considerations (NATO CCDCOE, 2010), p 18 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[3] "Cited from: Estland im Visier: Ist ein Internetangriff der Ernstfall?. Frankfurter Allgemeine Zeitung, 18.06.2007, Nr. 138 /Seite 6. (in German)", [3] Tikk, Kaska, Vihul, International Cyber Incidents. Legal Considerations (NATO CCDCOE, 2010), pp 18 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[4] Tikk, Kaska, Vihul, International Cyber Incidents. Legal Considerations (NATO CCDCOE, 2010), p 21 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[5] Tikk, Kaska, Vihul, International Cyber Incidents. Legal Considerations (NATO CCDCOE, 2010), p 24 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

ISSN 2345-0126 (online)

Not a single NATO defence minister would define a cyberattack as a clear military action at present".[1]

Stuxnet, a malicious form of software also known as *W32.Stuxnet worm,* was first reported on 17 June 2010 under the name *Rootkit.TmpHider*. *Stuxnet* targeted the computer systems of five facilities (according to recorded WAN IP addresses / computer domain names) located in Iran, between June 2009 and May 2010. The worm affected specific industrial control systems which use a type of software for management of large-scale industrial systems SCADA systems developed by the company Siemens and showing specific configuration requirements.[2]

According to *Stuxnet´*s architecture, the worm was created to amend the code of Programmable Logic Controllers (PLCs) of industrial control systems in order to amend the plant's operations by manipulating frequency converter control systems and thus slowing down or speeding up a motor, as well as hiding such changes from the operator of the respective equipment. Nuclear infrastructures in Iran as the targets of *Stuxnet*, namely the uranium enrichment plant at *Natanz* and/or the nuclear power plant at *Bushehr*, suspecting that the speed of the IR-1 centrifuges´ rotors was being amended in order to negatively affect Iran´s nuclear programme.[3]

Based on information available in media, it is not known whether *Stuxnet* did affect the physical integrity of IR-1 centrifuges or other components in Iran´s uranium enrichment plant at *Natanz*, the nuclear power plant at *Bushehr* or in other nuclear facilities. Iranian officials did not confirm any actual damage of a physical nature which had been caused by *Stuxnet*.[4]

In December 2015, Ukraine faced a major escalation in the seriousness of the Russian cyberattacks on its CEI.[5] According to the US Department of Homeland Security, which reported on the case, the Russian cyberattack on the Ukrainian CEI was one of the most successful cyberattacks on CEI in the world.[6]

Facts are the following. An unpredictable blackout of electric power occurred in several areas of Ukraine (Ivano-Frankivsk, Chernivtsi, Kyiv regions) on 23 December 2015, at about 4:30 in the morning. In that moment, a message appeared on the official website "Prykarpattiaoblenergo" (Ivano-Frankivsk region) about large-scale failures in the power supply system that occurred for unknown reasons. Immediately after the attack, it was discovered that the reason for stopping the work of the control equipment was an external intrusion into the operation of the power grid monitoring and control systems.[7]

---

[1] Tikk, Kaska, Vihul, International Cyber Incidents. Legal Considerations (NATO CCDCOE, 2010), p 24 http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[2] Katharina Ziolkowski, Stuxnet – Legal Considerations, (NATO CCDCOE, 2012, Tallinn), p 3, https://ccdcoe.org/multimedia/stuxnet-legal-considerations.html

[3] Katharina Ziolkowski, Stuxnet – Legal Considerations, (NATO CCDCOE, 2012, Tallinn), p 4, https://ccdcoe.org/multimedia/stuxnet-legal-considerations.html

[4] A denial of any physical damage by Iranian officials was reported by: Reuters, After Stuxnet: Iran says it's discovered 2nd cyber attack, in: The Jerusalem Post online available at http://www.jpost.com/IranianThreat/News/Article.aspx?id=217795

[5] "The first case of a successful cyberattack on energy objects has been registered in Ukraine" Ukrainian National News Link: http://www.unn.com.ua/uk/news/1552689-minenergovugillya-pershiy-u-sviti-vipadok-vdaloyi-kiberataki-na-obyekti-energetiki-zareyestrovano-v-ukrayini

[6] US DHS ISC-CERT Alert Link: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[7] Plėta, T., Karasov, S., Jakštas, T. 2018. The means to secure critical energy

ISSN 2345-0126 (online)

Simultaneously, hackers struck a powerful blow to the computer networks of the energy company "Kyivoblenergo". The hackers managed to access the IT systems controlling the substations of the company by temporarily disrupting the electricity supply to end consumers.[1]

To summarize, the interrupted power supply led to the disconnection of 220 thousand consumers between 1 to 3.5 hours. It should be noted that a shutdown did not cause serious damage to the electricity system of Ukraine. It was a loss 73 MWhrs (0.015% of electricity consumption per day).[2]

After the cyberattack on Kyivoblenergo, some others followed. For instance, the "North" substation of 330 kV (NEC "Ukrenergo") was completely de-energized on 17 December 2016. This resulted in the outage of a load of 144.9 MW for the "Kyivenergo" Public Company (Kyiv City) and of 58 MW for another company, "Kyivoblenergo" (the Kiev region). A Kyiv pump-storage plant was also de-energized with a loss of in-house supply.[3]

According to some analysts the attack was more sophisticated but was not fully exploited (attackers had the power to do worse) and may have been just a "test" of a new capability.[4]

Consequences and effects of cyberattacks on CI and right self-defense in light Article 5 of NATO Treaty

In the analysis and literal interpretation of Article 5 of NATO Treaty it becomes clear that these norms do not foresee consequences in terms of content. However, take in account opinion of ICJ[5] that the scale and effects required for an act to be characterized as an armed attack, it should be focus on such elements of "Armed Attack" as consequences.

If a cyberattack leads to a significant number of fatalities or causes substantial physical damage or destruction to vital infrastructure, military platforms or installations or civil property, it could certainly be qualified as an 'armed attack' within the meaning of Article 5 of NATO Treaty. A digital attack against information systems linked to vital infrastructure, military installations and platforms for weapons systems or vital services, such as the emergency services or air traffic control

---

infrastructure in the context of hybrid warfare: the case of Ukraine, *Journal of Security and Sustainability Issues* 7(3): 570. http://doi.org/10.9770/jssi.2018.7.3(16)

[1] Vytautas Butrimas NATO ENSEC COE. Cyber-attack on UKRAINE'S CEI (2015) Case Study, Energy Security Awareness Course, Tbilisi, Georgia, 26 April 2017.

[2] Vytautas Butrimas NATO ENSEC COE. Cyber-attack on UKRAINE'S CEI (2015) Case Study, Energy Security Awareness Course, Tbilisi, Georgia, 26 April 2017.

[3] Threat Intelligence Report, Cyberattacks against Ukrainian ICS. The views expressed by V. Butrimas are for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. Link: https://www.sentryo.net/wp-content/uploads/2017/09/EBOOK_CYBERATTACKS-AGAINST-UKRAINIAN-ICS.pdf

[4] Threat Intelligence Report, Cyberattacks against Ukrainian ICS. The views expressed by V. Butrimas are for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. Link: https://www.sentryo.net/wp-content/uploads/2017/09/EBOOK_CYBERATTACKS-AGAINST-UKRAINIAN-ICS.pdf

[5] Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, para. 195, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

ISSN 2345-0126 (online)

systems, could breach the threshold of an armed attack if it causes significant loss of life or physical destruction.[1]

Consequently, neither the attacks on Estonia in 2007 nor *Stuxnet* on Iran in 2010 and Ukraine in 2015, 2016 fall within the definition of armed attack. Those attacks did not cause any human or material damage and the disruption that they did cause was contained and was manageable.

However, from opinion of Benedetto, the first approach leaves out cyberattacks that have serious consequences without actually causing physical damage, destruction, injury or death. Consider for example a cyberattack that targets the financial system of a State or other CI, such as SCADA networks, severely affecting the functioning of a State or even causing a State to be paralyzed. It appears disproportionate that these cyberattacks would not reach the threshold of armed attack, while their effects may be more severe, long lasting and on a greater scale than other effects caused by traditional armed attacks. [2]

Others experts took the view that it is not the nature (injurious or destructive) of the consequences that matters,[3] but rather the extent of the ensuing effects.[4] Roscini suggested that in order for a cyberattack to amount to an armed attack, it has to be a use of force first, such an operation that causes or is reasonably likely to cause extrinsic physical damage to persons or property or severe disruption of critical infrastructures, in spite of a contrary opinion.[5] Dinstein has suggested some examples of cyberattacks serious enough to amount to "Armed Attacks" without extrinsic physical damage to persons or property.[6]

NATO member countries such as the United States and the Netherlands indicate what the criteria could be for a cyberattack without physical consequences to constitute an "armed attack."[7]

Cyberattacks can produce multiple effects. *The primary effects* are those on the attacked computer, computer system or network, the deletion, corruption, or alteration of data or software, or system disruption through a DDoS (Distributed Denial of Service) attack or other cyberattacks. *The secondary effects* are those on the infrastructure operated by the attacked system or network (if any), its partial or total

---

[1] Cyber Warfare, No 77, AIV / No 22, CAVV December 2011, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[2] Enrico Benedetto Cossidente, " Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO ", *NATO Legal Gazette* 61, 35 (2014): 32, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

[3] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* UK: Cambridge University Press, 2017, 342.

[4] Advisory Council on International Affairs, Cyber Warfare, No. 77, AIV / No 22, CAVV, at 21 (December 2011) (stating the implied approval by the Netherlands of the position that: 'if there are no actual or potential fatalities, casualties or physical damage', a cyber operation targeting 'essential functions of the state could conceivably be qualified as an "armed attack" . . . if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state.'), https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

[5] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 71.

[6] "Cited from: Dinstein, 'Computer Network Attacks', p 105", Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 73.

[7] Florentine J.M. de Boer, " Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defence Policy", *NATO Legal Gazette* 61, 35 (2014): 33, http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

destruction or incapacitation. *Tertiary effects* are those on the persons affected by the destruction or incapacitation of the attacked system or infrastructure, for instance those that benefit from the electricity produced by a power plant incapacitated by a cyber operation.[1]

The 2011 AIV/CAVV Report on Cyber Warfare, the *jus ad bellum* conclusions of which have been endorsed by the Dutch government, states that "a serious, organized cyberattack on essential functions of the state could conceivably be qualified as an 'armed attack' within the meaning of articles 5 of NATO Treaty and 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state".[2]

Thus, the author agrees that the consequences and effects of cyberattacks are of a diverse nature. The presence of serious damage, destruction or death is not mandatory, it is enough to disrupt the functioning of the CI of the state for a sufficiently long period, which may entail further serious consequences. Also, the author found a difference in views on such approaches of NATO member states. A single approach within NATO is necessary, its form can be different.

Conclusions

To conclude the analysis of the meaning cyberattacks as "Armed Attacks" on the objects of critical infrastructure in light article 5 of NATO treaty author come forward with the following points:

1. The objects of the cyberattack can be either military and civilian, government or private, even situated outside the State's territory. When it comes to cyberattacks, in most cases they are conducted on CII, which is directly connected to the automatic control of critical infrastructure.

2. Cyberattacks as "Armed Attack" can be with consequences as physical damage, destruction, injury or death and without of such consequences if it significantly affects the performance of State functions in various sectors of security, defense, economy, and society.

3. As a result of a legal analysis of the consequences and effects of an armed attack, it can be assumed that the case in Estonia in 2007 reaches the level of an armed attack in light Article 5 of NATO Treaty. Although cyberattacks during of 3 weeks did not cause serious destructive damage to the state, however, created a negative economic, informational and social effect during this a long period. This was not allowed to perform state functions.

4. The case *Stuxnet* in Iran in 2010 shows not clarity in the consequences and the effects after a seriously organized cyberattack. Similarly, the cyberattack did not create long-term destruction or termination of CI and does not reach the level of an armed attack.

5. Cases in Ukraine in 2015, 2016 should be seen as a cyber company that consisted of several cyberattacks on CEI. However, the consequences, unlike Estonia,

[1] Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014), 52-53.
[2] Cyber Warfare, No 77, AIV / No 22, CAVV December 2011, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

were not prolonged or destructive and thus did not reach the level of an armed attack. This led to a criminal investigation at the national level.

References

A denial of any physical damage by Iranian officials was reported by: Reuters, After Stuxnet: Iran, http://www.jpost.com/IranianThreat/News/Article.aspx?id=217795

Among others, the foreign minister of the Russian Socor, Vladimir. 'Moscow stung by Estonian ban on totalitarianism's symbols'. Eurasia Daily Monitor, The Jamestown Foundation, 26 Jan 2007, http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=32427

Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), 27 June 1986, http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Critical Infrastructures Protection Act of 2001, the United States, https://www.govtrack.us/congress/bills/107/s1407/text

Cyber Warfare, No 77, AIV / No 22, CAVV December 2011, https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf

Dinstein, 'Computer Network Attacks',

Enrico Benedetto Cossidente, " Legal Aspects of Cyber and Cyber-Related Issues Affecting NATO ", NATO Legal Gazette 61, 35 (2014), http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

Final Evaluation Report, Advanced Training Course on Critical Energy Infrastructure Security with Tabletop Exercise Coherent Resilience (CORE) 2017, NPS EAG, Kyiv, Ukraine.

Florentine J.M. de Boer, " Examining the Threshold of "Armed Attack" in light of Collective Self-Defence against Cyber Attacks: NATO's Enhanced Cyber Defence Policy", *NATO Legal Gazette* 61, 35 (2014), http://www.act.nato.int/images/stories/media/doclibrary/legal_gazette_35.pdf

For a comprehensive technical analysis of Stuxnet, see Symantec's Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, version 1.4, February 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

infrastructure in the context of hybrid warfare: the case of Ukraine, Journal of Security and Sustainability Issues 7(3) http://doi.org/10.9770/jssi.2018.7.3(16)

Katharina Ziolkowski, *Peacetime Regime for State Activities in Cyberspace, International Law, International Relations and Diplomacy* (Tallinn, Estonia: NATO CCD COE Publications, 2013)

Katharina Ziolkowski, Stuxnet – Legal Considerations, (NATO CCDCOE, 2012, Tallinn), https://ccdcoe.org/multimedia/stuxnet-legal-considerations.html

Limba T.; Plėta T.; Agafonov K.; Damkus M. 2017. Cyber security management model for critical infrastructure, Entrepreneurship and Sustainability Issues 4(4), http://dx.doi.org/10.9770/jesi.2017.4.4(12)

Marco Roscini, *Cyber Operations and the Use of Force in International law* (UK: Oxford University Press, 2014)

Michael N. Schmitt, Tallinn *Manual 2.0 on the International Law Applicable to Cyber Operations*, UK: Cambridge University Press, 2017,

National cyber security strategy Finland's Cyber Security Strategy (2013), https://ccdcoe.org/cyber-security-strategy-documents.html

National cyber security strategy of Lithuania, Programme for the Development of Electronic Information Security for 2011–2019 (2011), https://ccdcoe.org/cyber-security-strategy-documents.html

NATO Cooperative Cyber Defence Centre of Excellence, Tallinn , Estonia, says it's discovered 2nd cyber attack, in: The Jerusalem Post online available at https://ccdcoe.org/cyber-definitions.html

Plėta, T., Karasov, S., Jakštas, T. 2018. The means to secure critical energy

The first case of a successful cyberattack on energy objects has been registered in Ukraine" Ukrainian National News Link: http://www.unn.com.ua/uk/news/1552689-minenergovugillya-pershiy-u-sviti-vipadok-vdaloyi-kiberataki-na-obyekti-energetiki-zareyestrovano-v-ukrayini

The first case of a successful cyberattack on energy objects has been registered in Ukraine" Ukrainian National News,

The North Atlantic Treaty, Washington D.C., 4 April 1949, https://www.nato.int/cps/en/natohq/official_texts_17120.htm

Threat Intelligence Report, Cyberattacks against Ukrainian ICS. The views expressed by V. Butrimas are for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals, https://www.sentryo.net/wp-content/uploads/2017/09/EBOOK_CYBERATTACKS-AGAINST-UKRAINIAN-ICS.pdf

Tikk, Kaska, Vihul, International Cyber Incidents. Legal Considerations (NATO CCDCOE, 2010), http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

US DHS ISC-CERT Alert Link: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Vytautas Butrimas NATO ENSEC COE. Cyber-attack on UKRAINE'S CEI (2015) Case Study, Energy Security Awareness Course, Tbilisi, Georgia, 26 April 2017.

Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, North Atlantic Council, para 72, 5 September 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en