REVIEW

Annals of Disaster Risk Sciences

Vol 3, No 2 (2020)

Historical Perspectives and Legal Aspects of Cyber Warfare

Zoran Jovanovski, Military academy Gen."Mihailo Apostolski", Skopje, R.N.Macedonia
Andrej Iliev, Military academy Gen."Mihailo Apostolski", Skopje, R.N.Macedonia
Anita Ilieva Nikolovska, Lexicographic Centre, Macedonian Academy of Sciences and Arts, R. N. Macedonia

Address for correspondence: Andrej Iliev, Military academy Gen."Mihailo Apostolski", Skopje, R.N.Macedonia, e-mail: andrej220578@gmail.com

Abstract

Historical development of cyber warfare follows three major historical periods: first period follows the technological advances of information technology during the 1980s until the end of the Cold War in 1990, second period is from the end of the Cold War to the terrorist attacks in United States during 11-th september 2001 year and the third period is from the terrorist attacks in United States during 11-th september 2001 year onwards. Each of the mentioned historical periods follows a specific doctrine and strategy of dealing with the national security threats from cyberspace. The world super powers and the world states, introduce appropriate strategies and national policies to deal with the consequences of this kind of warfare. Expression of cyberspace is linked to a short story titled "Burning Chrome" in the 1982 year written by American author William Gibson. In the following years, this word turned out to be conspicuously related to online PC systems. According to NATO, people are part of cyberspace. According to this, NATO defines that cyberspace is more than just internet, including not only hardware, software and information systems, but also peoples and social interaction with these networks. The first cyber warfare weapon ever known in history was Stuxnet. Stuxnet's objective was to physically annihilate a military target. Stuxnet has contaminated more than 60,000 PCs around the world, mostly in Iran. While international cooperation is essential, each nation should in near future develop a National foundation, its own national cyber security strategy, authorities and capabilities. Every nation state, should require effective coordination and cooperation among governmental entities at the national and sub-national levels as well as the private sector and civil society. The main hypothesis of this paper is to present the historical development and perspectives of cyber warfare and accordingly propose the best legal concepts, national doctrines and strategies for dealing with this modern type of warfare.

Keywords

historical development, perspectives, cyber warfare, national strategies, legal concepts

1. Introduction

The term "*cybercrime"* was firstly presented from author William Gibson in 1982 year, when he wrotes in his book "Neuromancer". This book become very popular because present and manages today's virtual reality and network information activity to readers in a practical or constructive way. The novelist William Gibson in a very simple way, defines *"cyberspace*" as a constructed virtual environment in which information or computer systems and networks have a dominant or primary role[1]. The term "cybercrime" has further symbolized the insecurity and security threats that come from Internet, actually through the information and communication networks and systems. Thus, these security threats coming from the virtual information

environment represent a breach of computer security. Cyber warfare as a new model of proxy war, represents the future of modern warfare. With continuous development of modern computer systems and networks, they represent a continuous proxy strategy for conducting modern cyber attacks. The high level of autonomy of computer systems and networks enables them to build an effective proxy warfare strategy in which the performer of these cyber operations is always in advantage over attacked side. On the other hand, implementing a proxy strategy of warfare over computer networks is a much simpler method than using sophisticated weaponry to perform the most sophisticated military operations. Numerous classical armies are no longer an integral part of proxy warfare. Continued development of information technology is a necessity for executing a proxy strategy in cyber warfare, which as a mode of warfare is increasingly a major segment of modern warfare such as hybrid and comprehensive or compound warfare. The attacks on critical infrastructure most often include: public gatherings, hospitals, shopping malls, infrastructures of strategic importance to national security, airports and other strategic facilities of the state and through vulnerability of their information and communication network, the enemy achieve a far more effective attack than by using numerous armed forces in which casualties could be numerous. When we summarize, all this in cyber warfare, where there is no use of military force, therefore we don't have casualties. The Center for Strategic and International Studies (CSIS) estimated that between May 2006 and June 2011 there were at least almost eighty ‘significant cyber incidents’ that had resulted in ‘successful attacks on government agencies, defense and high tech companies or economic crimes with losses of few million dollars[2]. Stuxnet is one of the most complex threats to information systems. The final goal of Stuxnet, is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. Stuxnet is a threat targeting a specific industrial control system like in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries[3]. Generally, cyber attacks are separated into three major categories: (I) ‘automated malicious software delivered over the Internet, (II) ‘denial-of-service attacks,’ and (III) ‘unauthorized remote intrusions into computer systems[4].

2. Historical development of cyber warfare

As we mentioned earlier in the paper, first period of historical development of cyberwarfare encompasses the technological development of information technology from early 1980s to the end of the Cold War in early 1990s. Here we will try to highlight the most important examples of cyber attacks and cyber operations during this decade. During 1982, US President Ronald Reagan approved a "state secret" plan for the use of specific software capable of controlling gas supply pumps and their turbines on industrial gas production and distribution facilities in the former Soviet Union. Fortunately or unfortunately, this software was stolen by secret Russian agents during their stay in Canada. This software was able to change the flow rate of the gas pumps and thereby succeeded in causing them to malfunction. Former US Air Force Secretary and former Director of the National Reconnaissance Office, Thomas C. Reed, in his book "At the Abyss: An Insider's History of the Cold War," says that the psychological effect from this software and the effect on the Soviet Union's economic capacities, significantly speed up the process of ending the Cold War. US use cyber warfare during Iraq's invasion in 1991 year[5]. During Operation Desert Storm, a strategic air campaign was launched against Iraq's air defense, so that the command and control telecommunications information system was attacked by advanced computer software, causing electrical disruptions in Iraq's telecommunications information system[6]. The second period of cyber warfare development is in the next decade from 1990 to the terrorist attacks on US during 11-th September 2001. After the end of the Cold War and the collapse of the Soviet Union in 1994 in Chechnya, a virtual online war broke out between Chechens and pro-Russian forces. This virtual war on the Internet simulates military operations which one or other party wants to carry out in the field in real sense.

This sophisticated Internet psychological propaganda, with such widespread actions in military terminology is known as psychological surgery. Finally, it was found that the psychological operations were expressed through web portals and online simulations as a segment of cyber warfare which were funded through bank funds in Sacramento, California, which greatly helped to united Chechen diaspora to end this cyber war as

soon as possible[7]. During the Second Russo-Chechen Cyber War from 1997 to 2001 year, numerous military records of assassinations of Chechen and Russian soldiers mounted on both sides appeared on Internet and official Russian and Chechen web portals to make it successful. That was internet psychological propaganda among the nations. What we can conclude below is that Chechens' Internet propaganda has proved more successful. Digital videos and pictures of how a civilian Chechen bus has been attacked by pro-Russian separatists and many of these passengers have been killed and the activities from ambushes by Chechen militias on Russian military convoys are just some of propaganda material on internet web portals during 1999 year, which were officially denied from Russia. Russian authorities, on the other hand, have been conducting cyber attacks by hacking Chechen websites. So, the Russian Federal Security Service (FSB), along with Russian Special Forces "Spetsnaz", was responsible for preventing two Chechen web portals from operating[8]. Kosovo crisis from 1999 year is considered as one of the first more sophisticated information wars. When NATO was prepare to carry out its air campaign in Serbia with bombing critical infrastructure targets in order to bring the country into collapse, thereby forcing Serbia to withdraw from Kosovo. During the preparations for the air strikes, numerous hacker groups emerged, notably the "Black Hand", which launches serious cyber attacks on NATO's official and secret Internet infrastructure. Unfortunately, it can't be confirmed with certainty, but is assumed that some of the hackers were from Yugoslav Army.

Their goal was more than clear - to disable NATO air military operations on critical infrastructure in Serbia. It is also assumed that NATO missile incident at the Chinese Embassy in Belgrade is definitely the work of Serbian hackers which manage the change of missile's flight coordinates from its launch to the target[9]. During September 2000 year, young Israeli hackers manage to hack several Hezbollah and Hamas websites in Lebanon. Young hackers attack the operating system of web portals and successfully penetrate and gave fake news in 6 web portals to: Hezbollah, Hamas and other organizations in Lebanon, as well as the Palestinian national authorities. This seemingly minor cyberattack escalated as international incident. Palestinian and other Islamic organizations call it "*Holy cyber war*"[10]. The hackers carried out cyber attacks on 3 high-ranking Israeli web sites belonging to the Israeli parliament, Foreign Ministry and Israeli Defense Forces. Later, they also launched a cyber attack on the office of Israeli Prime Minister, Bank of Israel and Tel Aviv Stock Exchange. By January 2001, the cyber conflict had affected more than 160 Israeli and 35 Palestinian major web portals. About 548 domains of Israeli websites were hacked in Middle East.

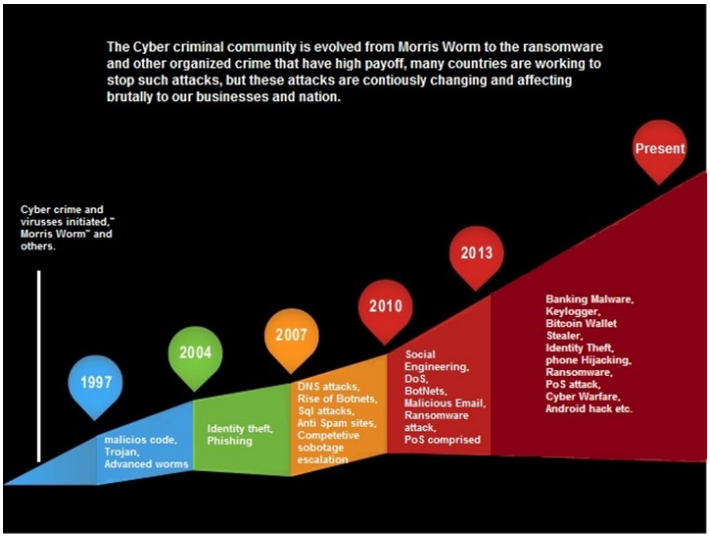

Figure 1. History of Cyber crime from 1997 till now
Source: https://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/#gref

The most common cyber attacks were web sites malfunctions and operating system attacks. Cyber attacks on telecommunication companies were also carried out. Palestinian hackers have succeeded in destroying Israel's NetVision, which supplied about 70 percent of national internet communications. The third and last historic period of cyber warfare begins after the terrorist attacks on United States from 11-th September 2001 year. The first significant cyberattack in the third historic period of cyber warfare was in Estonia in 2007. Estonia, as a small country with a population of over 1.3 million, has become a world-wide boom in the use of internet technology in a very short period of time. As a part of many advanced countries in

implementation of internet technology, Estonian government in November 2005 year, made whole Estonia as a virtual domain. The meetings at highest national level, other business meetings were conducted online, through virtual domain. Also the signing of documents were carried out with electronic signatures. Estonian citizens were able to vote electronically through their computers. Estonia was the 23rd country in the area of readiness and implementation of advanced information technology. Over 60% of the population had electronic bank accounts, while 95% of the bank transactions were made electronically. All of this, was tempting for the interest of numerous hackers to test Estonian cyber defense[11]. On 27-th April 2007 year, Estonian government relocated the monument of the victims of Soviet armed forces' liberation of Estonia from the fascist regime during World War II. The act of moving the monument from the center of Estonian capital Tallinn, outside the city, sparked with protests and clashes between Estonians and Russians. The protests were followed, with numerous cyber-attacks from Russian hackers targeting operating systems of national and private firms and enterprises. The main internet provider and Estonian government's website, which had a normal flow of 1000 emails per day, during the cyber attacks they received spam messages of 2,000 messages per second. The government network was designed to handle 2 million megabits per second and servers were flooded with nearly 200 million megabits per second during cyber attacks. The longest attack lasted over 10 hours and generated over 90 million megabytes of data per second. Because of this, the websites of Ministry of Foreign Affairs and Justice were shut down until the cyber attacks on websites were neutralized and restored. Banks in Estonia were closed, which in addition the national financial losses were also felt in international banking[12]. During 15-th May 2007 year, Russian hackers succeeded in disabling Estonia's national telecommunications information system E-112, although Estonian authorities have officially acknowledged, but Russian authorities refusing to admit it[13]. US and NATO have sent teams of computer security experts to help Estonian authorities to cope with the massive wave of attacks on operating systems that have paralyzed country's government websites, banking industry and media. What was of particular interest to computer security experts then, was that although the cyber attacks lasted for several weeks, their intensity was really high. The coordinated activities of NATO allies have for a short time stabilized the cyber security in Estonia. However, the websites of national authorities, State Office and Federal National Election Committee were also targeted by cyber attacks during May 2007 year. The British security service, office of French prime minister and office of German Chancellor Angela Merkel, have complained to China about cyber attacks on their government networks. Merkel even have raised the issue with Chinese president. So far, no official source in China has acknowledged involvement in this cyber attacks.

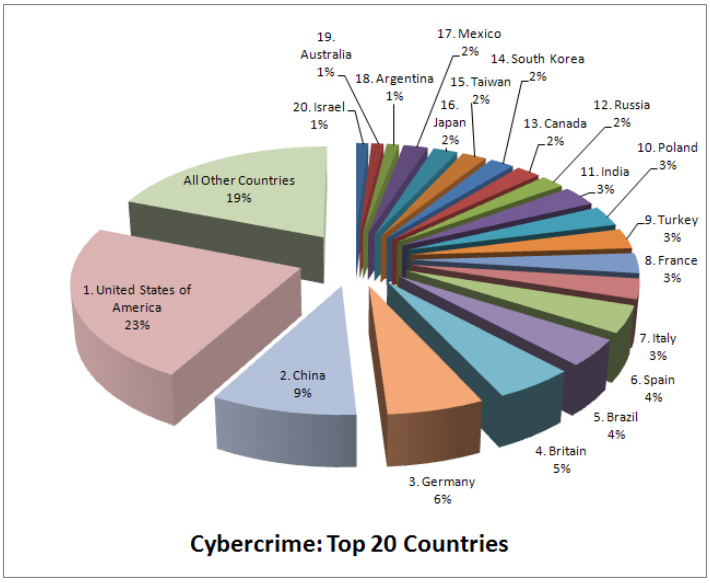

Figure 2. Top 20 world countries victims of cyber crime
Source: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

Cyber-worm called "*Stuxnet"* of unknown origin was developed and published in a number of countries in 2009 year, which damaged spin cascades and managed the Nantz's nuclear reactors in Iran. Stuxnet is a sophisticated cyber weapon. Attacks and disables nuclear centrifuges that works with SCADA system and exceed their sophisticated proprietary software and therefore are capable of overburdening centrifuges[14]. Expert estimates show that will took several years for development of classified information equipment and

type of cyber-worm that would be more sophisticated than commercial software, but estimates are that cyber attacks on the operating system would be successful. The nuclear power plants, which carried out cyber attacks must have access to highly restricted and classified information systems and equipment[15]. During 2011 year, Canadian government reported a major cyber attack against its agencies, including Defense Research and Development Canada, a research agency for Canada's Department of National Defense. The attack forced Canada's main economic agencies, to disconnect from the Internet. In July 2011 year, US Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the Department of Defense were stolen. The Russian firm Kaspersky during 2012 year discovered a worldwide cyber-attack dubbed "Red October," that had been operating since at least 2007. Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programs. The primary targets of the attack appear was Eastern Europe, former USSR and Central Asia, although Western Europe and North America reported victims as well. The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures. South Korean financial institutions in 2013 year were under cyber attacks, when Korean broadcaster YTN had their networks infected in an incident said to resemble past cyber efforts by North Korea[16].

3. Legal aspects of cyber warfare

Having in mind the historical development and perspectives of cyber warfare, what we know so far is that EU together with NATO developed cyber security strategy, over past few years all NATO and EU members have developed their own national cyber security strategies that are in coordination with European Commission and EU legislation and norms for NATO member states[17]. From the point of international law, Estonian cyber attack can be described as an 'unjust' cyber attack. Seen from the perspective of *jus ad bellum*, the attack lacked a sufficient just cause and was not undertaken in any meaningful sense as a last resort. From the perspective of the just conduct of hostilities – *jus in Bello* – the attack was utterly indiscriminate and disproportionate in its threat of harm, at least, when compared either to the harm Russia or its citizens allegedly were suffering, or any legitimate military objective that might have otherwise been under consideration. The cyber attack on Estonia led NATO to establish Cooperative Cyber Defense Center of Excellence (CCD COE) in Estonia in May 2008 year with a staff of 30 specialists which became operational in August 2008 year and is part of a NATO network of 13 accredited Centers of Excellence dedicated to training representatives from NATO member countries on "*Technically sophisticated aspects of NATO operations****[18]***." The CCD COE focus is on coordinating cyber defense and establishing policy for aiding allies during cross-jurisdictional attacks.

EU strategy for cyber security is based on five principles that will be priorities for the future of the EU. EU's official emphasizes that cyber security is equally important as security in the physical space. In accordance with the official text of the EU cyber strategy, most important five principles are the following:

- Achieving cyber resilience;

- Reducing cybercrime;

- Developing cyber defense policy and capabilities related to the Common Security and Defense Policy (CSDP);

- Develop industrial and technological resources for cyber security and

- Establish a coherent international cyberspace policy for EU and promote core EU values[19]. During 2016 year EU-NATO collaboration started to take shape. At the summit in Warsaw, Presidents of the European Council, European Commission and NATO's Secretary General signed a joint declaration for better security cooperation between the institutions. The Joint Declaration emphasized seven categories for cooperation between NATO and the EU. Two were directly applicable to cyber defense: countering hybrid threats and cyber security and defense[20]. NATO and EU are facing with cyber security threats they intensive the advantages of cooperation and they current approach to cyber defense[21]. EU Task Force as a product of this cooperation developed three phases for strengthening EU cyber defense capabilities as follows:

- Base Case: Implementing 2017 Cyber Security Package and EU cyber security strategy from 2018;

- Establishing a Cyber Defense Coordinator;

- Creating a Cyber Defense Agency;

The final goal was creating Cyber Defense Agency. Creating of this Agency was made with following five stages:

- Implementation of NATO and EU Cyber Security Package from 2017 according to EU cyber strategy from 2018 and Cyber Defense Policy Framework;
- In coordination with ENISA, EU Commission alongside other agencies such as the EDA to create a Cyber Defense Coordinator;
- Under the guidance of Coordinator and through prominent collaboration with industry, implement a series of cooperation-oriented tasks that would lead to development of a technical attribution forum;
- Under the guidance of Coordinator, investigate and draft the mandate of governance model for a Cyber Defense Agency Stage;
- Creating a Cyber Defense Agency that encompasses the coordinating functions of the Coordinator, ENISA's advisory capacity developed under 2017 Package and specific, core executive functions[22].

During 2019 EU Commission gave its recommendations to European Agency for Cyber security (ENISA) for cyber security of modern 5G networks this toolbox includes:

- An inventory of the types of security risks that can affect the cyber security of 5G networks (e.g. supply chain risk, software vulnerability risk, access control risk, risks arising from the legal and policy framework to which suppliers of information and communications technologies equipment may be subject in third countries) and

- Set of possible mitigating measures (e.g. third-party certification for hardware, software or services, formal hardware and software tests or conformity checks, processes to ensure access controls exist and are enforced, identifying products, services or suppliers that are considered potentially not secure, etc.).

These measures should address every type of security risk identified in one or more Member States following the risk assessment. Member States of EU together with the EU Commission, should identify the conditions concerning the security of public networks against unauthorized access to be attached to the general authorization and security requirements for networks for the purposes of asking commitments from the undertakings participating in procedures for granting rights of use of spectrum in 5G bands pursuant to Directive 2002/20/EC.

EU Member States should cooperate with EU Commission to develop specific security requirements that could apply in the context of public procurement related to 5G networks. This should include mandatory requirements to implement cyber security certification schemes in public procurement insofar as such schemes are not yet binding for all suppliers and operators. EU Members should cooperate with the EU Commission to assess the effects of this recommendation by 1 October 2020 year, with a view to determine appropriate ways forward[23]. This assessment should take into account the outcome of coordinated EU risk assessment from cyber threats.

4. Conclusion

One of the three most powerful states in the world, the United States through its government, sponsored website Cyber Seekers constantly advertises for cyber security job openings in United States that can be searched by state, city and so on. New roles and jobs in cyber security arise beyond the typical job roles. More interactive information, knowledge and sharing experience could be found on US National Initiative for Cyber Security Education (NICE) website. With the rapid development of information technology, it is more than necessary for government and private sector employees to be educated and trained in the field of cyber attack management and in implementation of appropriate legal regulations and mechanisms for legal protection and cyber attack sanctions. NATO Computer Incident Response Capability (NCIRC) upgrade project from 2013 year from 58 Million euro for enhancement of NATO cyber defense. This major capability will help NATO for better protection of its networks from increasing number of cyber attacks against Alliance's information systems.

So far, as initial example for other world states, the US government has established National Institute for Cyber security Education (NICE). NICE together with the Department of Education and other agencies launched a four-prong strategy to build a cyber secure nation through: training, awareness, post-graduate educational programs and development for federal security professionals. For meeting this goal, NICE targeted a wide array of population as prospective employees: students and private sector partners[24]. Cyber security reform legislation should make these arrangements permanent. Governmental agencies should be given the authority and resources to initiate new recruitment and education campaigns and extend scope of existing ones.

First, for increasing connectivity, more cyber security will be needed to manage that connectivity, so there will be a parallel increasing in demand for cyber security jobs. Second, through enhancing its presence in recruitment and education, federal government could attract those individuals to take a part of these cyber security jobs who might otherwise have joined the ranks of Anonymous or other hacker groups. Granted, persons who are anti-government or even apathetic towards government may not be persuaded from government's recruitment efforts. But for those young people who exhibit exceptional computer skills and seek a community which utilizes and appreciates these skills, the recruitment and education campaigns will certainly aid governments in this mission. The need for cyber security professionals is increasing day by day. The driving factors for this are: increasing number of useful internet and social networks, use of smart phones, electronic commerce of most financial and industrial corporations and more. All of this above mentioned increases the interest in cyber attacks on information systems and networks, especially on large financial and industrial corporations, whose dysfunction has only been negatively affected not only on a national but also on regional level, especially on the most powerful states in the world which for example: exports electricity, natural gas, petroleum products and so on. Many scientific papers point out that there is a shortage of staff, especially for high quality cyber security professionals. NATO is setting up a new Cyber Operations Centre in Mons, Belgium. The Centre will be fully operational in 2023 year. It will support the military commanders with situational awareness to inform the operations and missions and strengthen NATO's cyber defense. The centre will also coordinate NATO's operational activity in cyberspace ensuring the freedom to act in this domain and making NATO operations more resilient to cyber attacks[25]. International Information System Security Certification Consortium (IISSCC)^2 survey states that the cyber security workforce gap is on pace to hit 1.8 million by 2022 year[26].

5. References

Artur Appazov. Legal aspects of cyber security, University of Copenhagen, 2014.

Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer", *Bosnian Serb News Agency SRNA*, 28 March 1999.

Clay Wilson, Botnets. Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress, 2008.

Cyber War Also Rages in Middle East, *The Associated Press*, 28 October 2000.

Cyrus Farivar. "Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat," *Slate*, May 22, 2007.

David E. Hoffman, "CIA slipped bugs to Soviets," *Washington Post*, 2004.

Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn, Cooperative Cyber Defense Centre of Excellence (CCD COE),2010.

David S. Wall. cybercrime: The transformation of crime in the information age, Polity press - Cambridge, 2007.

European Commission. Cyber security of 5G networks, Strasbourg, 26.03.2019.

European Commission. Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 2013.

European Union External Action Service “EU-NATO cooperation – Factsheet” (https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-natocooperation-factsheet_en).

Gustav Lindstrom, Thierry Tardy. The EU and NATO essential partners, European institute for security studies, Brussels, 2019.

Jaap de Hoop Scheffer. Strengthening the EU’s Cyber Defense Capabilities Report of a CEPS Task Force, Centre for European Policy Studies (CEPS), Brussels, November 2018.

James A. Lewis, *The “Korean” Cyber Attacks and Their Implications for Cyber Conflict*, Center for Strategic and International Studies CSIS, October 2009.

Jose Nazario, Politically Motivated Denial of Service Attacks, Arbor Networks, 2009.

Mathhew J. Sklerov, Solving the Dilemma of State Responses to Cyber attacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 Military Law Review, 2009.

National cyber strategy of USA, USA, September 2018.

National Initiative for Cyber security Careers and Studies, “NICE Cyber security Workforce Framework,” USA, 12 December 2017.

NATO Cooperative Cyber Defense Centre of Excellence, Tallinn Manuel Process.

Nick Hopkins. China “Targets NATO Chief” in Facebook Spying Operation, Observer, 11 March 2012.

Nicolas Falliere, Liam O Murchu, Eric Chien. W32.Stuxnet Dossier, Symantec Corporation, USA, 2010.

Oliver Bullough. Russians Wage Cyber War on Chechen Websites, *Reuters*, 2002.

Operation Desert Storm: Evaluation of the Air Campaign, U.S. Government Accountability Office, Letter Report, GAO/NSIAD-97-134, 1997, Appendix V.

Steven Adair, Korean/US DDoS Attacks – Perplexing, Disruptive, and Destructive, 22. Shadow Server Foundation Calendar blog, 10 July 2009.

Timothy L. Thomas, “Information Warfare in the Second Chechen War: Motivator for Military Reform?”, Foreign Military Studies Office, Fort Leavenworth, 2002.

Internet resources:

1. https://resources.infosecinstitute.com/evolution-in-the-world-of-cyber-crime/#gref
2. https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/
3. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf
4. https://niccs.us-cert.gov/workforce-development/cyber-security-force-framework
5. https://ccdcoe.org/research/tallinn-manual/
6. https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-natocooperation-factsheet_en
7. https://www.thinkoutcyberbox.com.au/

[1] David S. Wall. (2007). Cybercrime: The transformation of crime in the information age, Polity press - Cambridge, 221-223.

[2] Nick Hopkins. (2012). China “Targets NATO Chief” in Facebook Spying Operation, Observer.

[3] Nicolas Falliere, Liam O Murchu, Eric Chien. (2010). W32.Stuxnet Dossier, USA,1-3.

[4] Mathhew J. Sklerov. (2009). Solving the Dilemma of State Responses to Cyber attacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent, 201 Military Law Review.

[5] David E. Hoffman. (2004). CIA slipped bugs to Soviets, *Washington Post*, 27.

[6]*Operation Desert Storm. (1997). Evaluation of the Air Campaign*, U.S. Government Accountability Office, Letter Report, GAO/NSIAD-97-134, Appendix V.

[7] Timothy L. Thomas. (2002). Information Warfare in the Second Chechen War: Motivator for Military Reform?", Foreign Military Studies Office, Fort Leavenworth, Kansas.

[8] Oliver Bullough. (2002). Russians Wage Cyber War on Chechen Websites, *Reuters*.

[9] *Bosnian Serb News Agency SRNA.(1999).* Yugoslavia: Serb Hackers Reportedly Disrupt US Military Computer.

[10] *The Associated Press*. (2000). Cyber War Also Rages in Middle East.

[11] Cyrus Farivar.(2007).Cyberwar I. What the Attacks on Estonia Have Taught Us About Online Combat," *Slate*.

[12] Clay Wilson, Botnets.(2008). Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress, Congressional Research Service Report for Congress.

[13] Eneken Tikk, Kadri Kaska & Liis Vihul. (2010). *International Cyber Incidents: Legal Considerations*, Tallinn, Cooperative Cyber Defense Centre of Excellence (CCD COE),15-34.

[14] Jose Nazario. (2009). Politically Motivated Denial of Service Attacks, Arbor Networks,8-12.

[15] James A. Lewis. (2009). *The "Korean" Cyber Attacks and Their Implications for Cyber Conflict*, Center for Strategic and International Studies CSIS, 9-11.

[16] Steven Adair. (2009). Korean/US DDoS Attacks – Perplexing, Disruptive, and Destructive, Shadow Server Foundation Calendar blog.

[17]Artur Appazov. (2014). Legal aspects of cyber security, University of Copenhagen, 38-42.

[18] NATO Cooperative Cyber Defense Centre of Excellence, "Tallinn Manuel Process," https://ccdcoe.org/research/tallinn-manual/

[19] European Commission. (2013). Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 4-5.

[20] European Union External Action Service "EU-NATO cooperation – Factsheet" (https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-natocooperation-factsheet_en).

[21] Gustav Lindstrom. (2019). Thierry Tardy. The EU and NATO essential partners, European institute for security studies, Brussels, 37-41.

[22] Jaap de Hoop Scheffer. (2018). Strengthening the EU's Cyber Defense Capabilities Report of a CEPS Task Force, Centre for European Policy Studies (CEPS), Brussels, 65-67.

[23] European Commission. Cyber security of 5G networks, Strasbourg, 26.03.2019, 7-8.

[24] National cyber strategy of USA. (2018). USA, 5-8.

[25] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902 cyber-defence-en.pdf

[26] National Initiative for Cyber security Careers and Studies, “NICE Cyber security Workforce Framework,” USA, 12 December 2017, https://niccs.us-cert.gov/workforce-development/cyber-security-force-framework