A New Field Between Two Old Allies: Cybersecurity Approaches of EU and NATO (2016-2020)

Eski İki Müttefik İçin Yeni Bir Alan: AB ve NATO'nun Siber Güvenlik Yaklaşımları (2016-2020)

Fatih Başar KUTLU*

* Milli Savunma Üniversitesi Atatürk Stratejik Araştırmalar Enstitüsü (ATASAREN) Uluslararası İlişkiler ve Bölgesel Çalışmalar Anabilim Dalı Yüksek Lisans Öğrencisi.

E-mail: f.basarkutlu@gmail.com

ORCID: orcid.org/0000-0003-2243-5606

Abstract

In this article we will analyze the approach of two well-known allies, NATO and EU, to a new dimension, Cyberspace, which brought a perspective to International Relations, and will try to understand how it could affect the relations between these organizations while there remains the conventional problems such as non-dual members and duplication of structures. Cyberspace, due to its nature, requires a well-organized and coordinated attitude to prevent damage that can be caused by malevolent actors through this new dimension. Therefore, nations and security organizations, The European Union and North Atlantic Treaty Organization in our case, should first get familiar with the nature of this dimension and following this must create a rapidly working information sharing and development web between like-minded actors. In this sense, we will also try to discuss the common threats according to these two like-minded organizations and finally point out the possible solutions against these threats.

Keywords: EU, NATO, Security, Cyberspace, Cyber Security.

Öz

Literatürde genel kabul gördüğü üzere NATO ve Avrupa Birliği (AB), ikili üyelik sorunu ve organizasyonel yapıda çakışma gibi geleneksel sorunlar yaşayan iki önemli örgüttür. Bu geleneksel sorunlar dışarıda bırakılarak çalışmada her iki örgütün "siberuzay" yaklaşımları incelenerek, süregelen ilişkilerini nasıl etkilediği analiz edilecektir. Bilindiği üzere siberuzay, doğası gereği olası zararları önleyebilmek adına katkı veren devletlerin yüksek bir uyum içinde ve ortak hareket etmesi gerek bir özelliğe sahiptir. Dolayısıyla NATO ve AB'nin de siberuzayda benzer güvenlik kaygılarına sahip aktörler olarak hızlı bir şekilde işleyebilecek bilgi paylaşımı ve gelişim ağı kurması gerekmektedir. Kuruluş değerleri bağlamında ortak birçok paydaya sahip olan bu iki organizasyonun güvenlik planlamalarında da ortak hareket etmelerinden daha doğal bir durum beklenemez. Zira siberuzay, insanlığın gelişimini destekleyebilecek şekilde barışçıl amaçlarla kullanılabileceği gibi değişen ve gelişen savaş boyutları bağlamında barışçıl olmayan amaçlarla da kullanılabilmektedir. Bu bağlamda çalışmada NATO ve AB'nin "siberuzay" stratejileri inceledikten sonra, aktörler arasındaki sorunlara muhtemel çözüm önerileri getirilecektir.

Anahtar Kelimeler: AB, NATO, Güvenlik, Siberuzay, Siber Güvenlik.

To Cite This Article/Bu Makaleye Atıf İçin: Kutlu, F. B. (2023). A New Field Between Two Old Allies: Cybersecurity Approaches of EU and NATO (2016 – 2020). Journal of Diplomatic Research, 5(1),

Research Article/Araştırma Makalesi

Makale Gönderilme Tarihi: 26.07.2023
Makale Kabul Tarihi: 21.08.2023

Introduction

Last two decades has been a great opportunity for emerging technologies to reach its peak point. While on the one hand they create an easier and more interactive future for us with facilitating our daily lives, on the other hand they are revealing new contexts to take advantage of, for malevolent actors. Besides, our lives now have been almost twenty-four hours of interaction with artificial intelligence.

Emerging technologies are also serving as a backbone of any country in a manner of political, economic and military development. Not just as an additional tool but more as an essential requirement of well-continuity.

In fact, integration of those systems which in total can be named as "Cyberspace" goes deeper and more developed in time with getting integrated with states' daily functions. Hence, they also attract attention of rogue actors.

Through time, this integrity and advancement also brought the requirement of a multidisciplinary approach to cyberspace instead of an old-minded technical understanding. Therefore, conventional actors of international system, such as NATO and the EU, and their long-term relation which currently including cyber security issues are also examined under cyber security studies. Nowadays, as it is not a matter of possibility but a matter of time to welcome a cyber-attack, integrity of state and commercial actors and international cooperation has become an obligation for all mentioned actors in sense of getting prepared more comprehensively.

In this regard, we will examine two dominant actor and organization of western world, namely NATO and the EU in separated chapters of this article first and their relation with also mentioning the effects of conventional long-lasting relations of those actors later. But in order to provide a sufficient base knowledge priorly, we will mention the definition and some important concepts of cyberspace and exemplify it with infamous incidents.

1. Importance and Definition of Fundamental Concepts

It is possible to say that, in the last decades, humanity developed such tools that speed of such development was incomparable with previous centuries. Although, nowadays reaching the internet is as simple as calling a service provider, creation and progress of development of such widespread network was established between four state computers in United States. Due to the advantage of fast processing, storing and transferring any information between such systems, with these computers first network, namely, ARPANET (Advanced Research Projects Agency Network) was established between Los Angeles, California, Santa Barbara and Utah in 1969 by Defense Advanced Research Projects Agency (DARPA). (Gary, Jessica & Katherine, 2009: 10)

In a short period of time, ARPANET divided into two to serve research on the one side and to military service on the other. Military service network (MILNET), however, needed more security measures which provided through transfer protocols (Transmission Control Protocol, TCP and Internet Protocol, IP). Protocols are set of rules that data transfer among devices happening through.

1.1. Definition of Cyberspace

This fast spread and mass use of the internet, as expectedly created a new sphere of information. Through time, as it passed through some phases called Web 1.0, 2.0 and 3.0 nowadays not only computers or smartphones are connected, but everything possible can be connected to the internet and created its ultimate form which called "Internet of Things".

While this enormous sphere generates a great opportunity to ease our life, on the other hand, creating possible new threats to our personal data, bank accounts and beyond us, composing danger also in national security levels. Although there is still no commonly accepted definition of this sphere, currently, the concept "Cyberspace" is being used to address it. The term now represents a new and less tangible dimension besides land, sea, air and space. Or as European Network and Information Security Agency (ENISA) defines; "Cyber space is the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information. " (European Network and Information Security Agency [ENISA], 2017)

Following four features of cyberspace, composes the distinctive nature of cyberspace from other dimentions: (Libicki, 2007:5)

- Replicability; unlike physical rules that binds outer space, existence of things in

cyberspace can be simultaneously exist in multiple locations,

- Different matter of existence; unlike other dimensions, in order to exist in cyberspace, actors are required to be linked and confirmed by each other or the related system;
- A unique aspect of cyberspace also creates its "unavoidably free" nature as it gives a new chance to illegal acts to have their own type of protocols.
- Finally, another separative characteristic of cyberspace is its three layered structure;
  - Physical layer; that consists of cables and devices,
  - Syntactic layer; that is formed by used instructions and controlling systems (such as software languages)
  - Semantic layer, which makes sense to users and interactions of users with the machine-generated information. (Libicki, 2009:11)

1.2. Fundamental Concepts

This forementioned unique characteristic of cyberspace and its role as a new dimension unavoidably brings out new concepts to understand its nature.

1.2.1. Cybersecurity

While security is defined as "*protection of a person, building, organization, or country against threats such as crime or attacks by foreign countries.*" in Cambridge Dictionary, the only difference seems to be the "*carried out using the internet*" addition for cybersecurity.

Although eventually attacks are required to be based on the internet, several different type of cyberattacks can also be carried out through offline means. In addition, as the main goal is to acquire information or access to required data through unauthorized ways, cybersecurity, expectedly, is related to information and network security. (Libicki, 2009:14)

In this context, ENISA (European Cybersecurity Agency with the final decision and European Network and Information Security Agency by its founding name) defines cybersecurity as preventing, envisaging, detecting, decreasing, examining and removing cyber incidents that happened or has the possibility to occur. Because the information and network security accepted as subsets of cybersecurity, besides integrity, availability and confidentiality; also reliability, safety, sustainability of physical layer, robustness, resilience, transparency, survivability, credibility, non-repudiativity are stated as attributes that a comprehensive cybersecurity structure should bear within.

1.2.2. Critical Infrastructure

Due to its crucial role for modernized societies, protection of those highly connected critical infrastructures inevitably becomes one of the significant necessities of cybersecurity.

What categorizes an infrastructure as critical is the possibility of having destabilizing or alike negative effects upon security, national economy, public health, public safety or any related subject, in case of any type of dysfunctionality happening to such critical systems or sectors. (CISA, 2020)

Due to its very nature and the purpose of creation, networking systems and cyberspace created as a result of it were already put forward in order to connect such infrastructures.

1.2.3. Cyberattacks

Cyberattacks, basically can be described as all possible malicious acts that are aiming to either disrupt or corrupt the integrity, availability and confidentiality of information networks, systems or directly the information. (Scott, 2017:31) While disruption of data deceives systems to act not in the way it is design so, such as instant shut downs, unexpected errors or possible interruptions of operation of other systems; corruption can be seen as a more cunning effect that although changes functioning way of data or algorithms of systems, such changes are made in a way that won't cause obvious effects and so will prevent awareness of the existence of corruption. Nevertheless, these or possible other effects of such attacks are not consequences of a "forced entry", instead, more possibly described as unauthorized entry by tricking related systems to "think" that ill-aimed attackers are authorized users. (Libicki, 2009:16) Here the importance of cyber hygiene shows up, because such attacks can only be possible by using opportunities granted by vulnerabilities, except insider attacks, that can also be accepted as tricking authorized users in order to help attackers.

1.2.4. Cyberwarfare

Cyber incidents could intentionally be created by hackers directly working for adversary nation-states or by attackers that are supported and sponsored by such states. However, due to relativity of the term war with physical violence and it is quite rare to see violent results of cyberattacks, (Green, 2015:1) in order to describe reciprocal cyberattacks made or sponsored by states, it is more appropriate to use the term "cyberwarfare".

Although, there are some critics against defining such type of incidents occurring in "virtual" cyberspace as "war" due to the low-level and isolated nature of it, experienced examples in last decades with even rare but possible consequences of causing physical damage, are revealing the increasing significance and unique nature of related subject. While exchange of attacks only occurring in cyberspace could be named as *strategic cyberwarfare* (Libicki, 2009:118), seeing it as a supportive another dimension can be called *operational cyberwarfare.* (Libicki, 2009:139)

2. European Union and Cyber Security

As explained above, continuing integrity of developed nations with cyberspace, reveals new vulnerabilities that could be used either for cybercrimes or to take advantage against those highly-integrated countries by their rivals. Hence it is possible to state that highly integrated societies need brand new understanding of security which, inevitably, comprehends cybersecurity measures.

EuroStat data is showing that internet usage percentage reaches out to almost a hundred percent in relatively developed nations such as the Netherlands, Iceland or Norway. (Eurostat, 2020) Besides significant wake-up calls to understand the necessity of cybersecurity measures such as Estonia and Kosovo examples are also showing the possibility of European soils to be taken as targets.

While currently, effort put forward by European Union is well-known with Network and Information Security Directive (NIS), General Data Protection Regulation (GDPR) and European Cybersecurity Agency (ENISA), which was first established as European Network and Information Security Agency; in this chapter we will examine the regulative and formative process of European Union through legal documents and official publications that Union has created between mentioned time period.

2.1. Pioneer Works

While societies were getting more dependent on technological development, especially during the last decade of 20. century, to have a united framework of many areas including security and some aspects of legislation, the EU took a step to regulate *" security of information systems"* for the sake of economic integration and harmonized development, in 1992.

With the Decision published by the Council (92/242/EC), mainly, importance of providing security to information systems and requirement of strategic framework developed under an action plan were emphasized. (European Council [EC], 1992) 3 years later, with the joint attendance of European Parliament and the Council published a directive *" on the protection of individuals with regard to the processing of personal data and on the free movement of such data"*. In fact, this directive can be taken as one of the first steps of currently active and well-known General Data Protection Regulation. (European Parliament [EP] & EC, 1995)

Following the previous work, on 12 July 2002, EP and the Council also established the directive *" concerning the processing of personal data and the protection of privacy in the electronic communications sector"* or Directive on privacy and electronic communications which extends the scope and comprehends also legal persons. (EP & EC, 2002) In this regard, it is possible to say that the Union was having its legislation more comprehensive day by day.

With the increasing and facilitating impact of digitalization, in 1999, Commission initiated eEurope program for the first time with the aim of spreading usage of emerging technologies all over the EU. In that sense, the main objectives were to enable EU citizens to access networks in their houses, schools, business and et. al.. With the eEurope- An Information Society For All program, requested in Lisbon 23-24 March 2000, the European Union for the first time initiated a program that we can identify as a general framework about information networks. Afterwards, eEurope program was followed by eEurope 2004 and i2010 programs that are adding new requirements occurred in time in the nature of information networks and emerging

technologies. (EC, 1999)

Following the adoption of the Europe Plan in the Feira European Council, Commission of the European Communities put another communication forward with the subject of " *creating a safer information society by improving the security of information infrastructures and combating computer-related crime*" to coordinate the fight against cybercrime. (EP & EC, 2001) Beside the cyberspace-based measures and methods, the problem of anonymity and non-legislative needs were also mentioned. Such as the proposal of EU Forum was a structure that consisted of law-enforcement representatives, internet service providers, telecommunication operators, civil society representatives, consumer representatives and data protection authorities.

Later in 2002, in order to extend the scope of progress that the EU has put forward to provide protection of its cyberspace and keep its citizens safe, the Commission has submitted another proposal " *for a Council Framework Decision on attacks against information systems*". With this proposal, the commission draws attention to increasing attacks against information systems and the rate of organized crime through means of emerging technologies. Following this proposal, the Council has adopted Framework Decision 2005/222/JHA on 24 February 2005 that carries the same title with the proposal.

In 2004, Commission with a communication once again extended the scope of protection of information systems and emphasized the importance of critical infrastructures especially in case of the fight against terrorism. In COM(2004) 702 Communication, while on the one side defining the term of critical infrastructure on the other side, the necessity of a general critical infrastructure protection program among the EU was underlined, namely the European Program for Critical Infrastructure Protection(EPCIP). Later in 2006 repeated once again with further details by COM(2006) 786 final Communication from the Commission " on a European Programme for Critical Infrastructure Protection". (European Commission [ECOM], 2006)

As some of the following work put forward in 2008 and 2009, in 2011, another communication presented by the Commission in order to show the achieved goals and to extend the scope of general protection of critical infrastructures, namely " *Achievements and next steps: towards global cyber security*" which the Commission once again underlined the importance of EU level of integration and cooperation for CIIP and danger of cyber incidents with no importance of either intentionally or not. (ECOM, 2011) Following this effort of Commission, in 2012, the Parliament broadly endorsed latter communication (EP, 2012) and these communications also drawed a general base for 2013 Cybersecurity Strategy. (ECOM, 2013)

2.2. European Network and Information Security Agency (ENISA)

In early 2004, several months before the establishment of aforementioned EPCI Program, due to requirement of a central organization that will provide sufficient support to coordinate national efforts and lead legislative work of the Union, with the initiative of the Parliament and the Council, European Network and Information Security Agency has been established with the Regulation 46/2004. (EP & EC, 2004)

In that sense, the main purpose of the Agency was described as establishing and preserving a high and effective level of security of European networks and information systems. With also provision of a general culture related to cybersecurity for sake of EU citizens and customers and flawless process of internal markets.

Even though the agency was established for only 5 years, laterly this period of time constantly extended and with the Cybersecurity Act, it has become a permanent organization. While this extension first made with Regulation No 1007/2008 until 2012, (EP & EC, 2008) with Regulation No 580/2011 another extension app. until September 2013 was foreseen. While Regulation No 526/2013 concerning the ENISA, provided more autonomy and financial support to the agency. (EP & EC, 2013) Finally in 2019 with the Cybersecurity Act, ENISA happened to be the main and permanent body of the union to provide sufficient support and effort needed in order to keep the Union's cyberspace safe. (EP & EC, 2019) Besides, the name of the agency was also changed into European Cybersecurity Agency (although the abbreviation kept the same).

Activities of ENISA have been considered under 3 categories: Expertise, Policy and Capacity.

2.3. The Cyber Security Strategy

In February 2013, just 3 months before the Regulation No 526/2013 on ENISA, the European commission created the Cybersecurity Strategy for the European Union with " An Open, Safe and Secure Cyberspace" slogan as part of the title. As the sophisticated nature of cyberspace gets more complicated day by day, the Commission determined the Cyber Security Strategy to be a general regulator and a framework. Also, the significance of regulating the digital market and creation of a Digital Single Market was emphasized in the strategy.

In that sense, main principles are stated as; (EP & EC, 2013: 1)

- Applying EU core values to cyberspace,
- Protection of fundamental rights, freedom of speech, privacy and personal data,
- Increasing availability of access to internet,
- Governing stakeholders democratically and efficiently,
- Ensuring security by sharing responsibility.

Forum appreciated in the first part of the Directive, it foresees further cooperation and development of a risk management culture among the Union. Besides, exercises focused on cybersecurity, such as Cyber Europe by ENISA, are stated as an important measure. Yet no regulative measures put forward related to hardware and software developers in the Directive. (EP & EC, 2016)

Responsibilities such as adopting a national strategy, identification of operators of essential services and updating this list per 2 years, creating national computer security incident response teams which will participate in the CSIRTs Network that is established with this directive, given to member states. Directive also asks member states to establish an authority which will work as a single point of contact and provide cooperation in transboundary cases. Designated competent authority shall supervise the process of adopting the directive in the national jurisdictional aspect.

2.5. CERT-EU

Following the adoption of the Digital Agenda for Europe in May 2010, initiatives by the Commission to establish a computer emergency response team at the Union level started. As

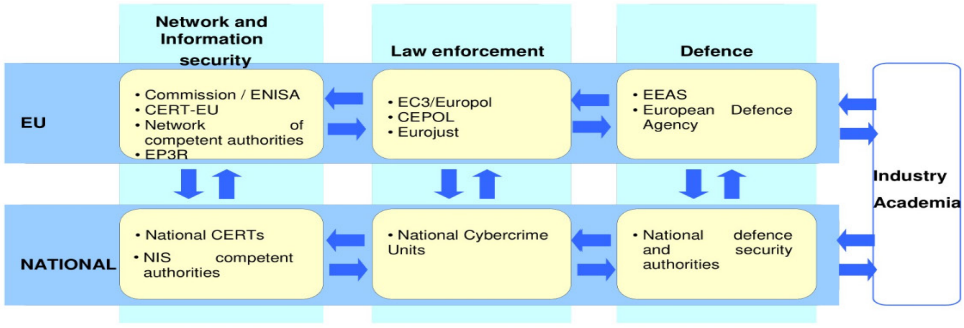

Figure 6: Three Key Pillars of Cybersecurity with Roles and Responsibilities in Cybersecurity

2.4. The NIS Directive

Following the attention paid by the Union to improve its cyber security, and the necessity of a general regulation about network and information security emphasized by several different documents repeatedly, in 2016, NIS Directive that determines what should be done by member states, service providers and operators of essential services was adopted by the Parliament, which is also the first EU-wide legislation related to cybersecurity.

Although the work put forward with the EU

this CERT-EU was found necessary to protect networks and information systems of the Union, the Commission asked recommendations from cybersecurity experts known as " Rat der IT Weisen" which translated into " Council of IT Wise Men". After the experts finalised their report upon the request, in November 2010, (The Computer Emergency Response Team EU [CERT-EU], 2020) the following year "Achievements and next steps: towards global cyber-security" adopted by the Union's Council of Telecom Ministers, which emphasizes the importances of and so calls for establishment of national

computer emergency response teams. (Council of the European Union [CoE], 2011) Finally, after a year of pilot phase, on September 11th 2012, the computer emergency response team for the European Union institutions, agencies and bodies was permanently set up.

While cooperating with national CERTs and also some companies related to information technologies security, the CERT-EU consists of cybersecurity experts from EU institutions. In order to meet the required conditions to prevent cyber incidents, in 2015 a new headquarters established for the team in accordance with increasing expertise and hence the respectability of the team.

And, finally, with the NIS Directive the Union established the CSIRTs Network.

2.6. The Cyber Security Act

Last but not least, one of the most recent and comprehensive regulations is the Cybersecurity Act which was also mentioned above in order to examine the changes it brought to the European Cybersecurity Agency. The Act stated the main problem of the Union in cybersecurity was the requirement of further measures due to the changing nature of cyberthreats and insufficient level of attention paid to the related works.

The fragmentation of legal approaches among the EU Members, insufficient level of awareness and information at the level of EU citizens and companies, and finally dispersed resources and handling between EU Institutions, Agencies and Bodies, determined as 3 main categories of the main problem of not properly acting as required and planned. (ECOM, 2017)

The Act consists of two main titles besides the general provisions and final provisions, which are; ENISA (The European Union Agency for Cybersecurity) and Cybersecurity Certification Framework. In order to avoid falling into repetition, here we will only take into consideration the latter as the first was explained above in the ENISA sub-title detailly.

Although there has been previous work for certification of ICT production, processing, and services, in order to have a more comprehensive and updated approach, a general European Cybersecurity Certification Framework was established with the act. (ECOM, 2017)

In this regard, certification process primarily aims to protect data, identify vulnerabilities, record data-logs and in case of incident, recover from the best possible point before damage geos further. Beside these, confirmation of ICT products' vulnerability-free and up-to-date software/hardware were also part of the certification process. While the certification was not determined to be obligatory and olders of the certificates are expected to inform related authorities in regard to vulnerabilities and irregularities which may have an impact on the compliance with related requirements. European Cybersecurity Certification Group which was established with the Act, held responsible for advising and assisting the Commission, ENISA, about related processes.

3. NATO and Cyber Security

As the significance and the capabilities of work possibly being done through cyberspaces grows in a short period of time rapidly, the military aspect was also made subject of such development of cyberspace. The North Atlantic Treaty Organisation (NATO) was targeted even before constant disturbance of the EU and expected to have further sophisticated cyberattacks due to aforementioned extension of cyberspace into the military aspect.

In this respect, while the first attacks were carried out in 1999, during the Kosovo Operation, it has revealed the significance of this new dimension for the Alliance. Further attacks occurred in 2007, against Estonia and the later use of cyberspace in Georgia in 2008 by Russian Military, as a part of a more complex hybrid-warfare techniques, emphasized the role and significance of NATO with increasing danger of cyberattacks.

Therefore, the Alliance created and extended its own cyber defence approach, starting with 2002 Prague Summit and still keeps cybersecurity measures as one of the main aspects of its security perception.

3.1. 2002 Prague Summit and NATO CIRC

During the NATO campaign to stop the ethnic cleansing in Kosovo, despite the superiority of NATO on conventional warfare, so called " nationalist" Serbians responded to such attacks with an unusual way of the time, namely,

through DDoS attacks. In this attempt, they were successful in blocking access to a variety of NATO web sites. The responsible Serbian hackers who were called " Black Hand" also tried to reach the NATO command servers and leak useful information, however, they could only break into networks of air forces, notwithstanding couldn't reach any useful information. (Szentgali, 2013)

Besides, due to bombing of the Chinese embassy in Belgrade, which was serving as a re-broadcasting station for the Milosevic's forces (Sweeney, Holsoe & Vulliamy, 1999), also Chinese hackers along with Serbian and Russians, were launching DDoS attacks. (Healey & Bochoven, 2012:1)

In this regard the Cyber Defence Program was adopted at the following NATO summit in Prague 3 years later. To detect such cyberattacks, to prevent and if required to respond, NATO Computer Incident Response Capability (NCIRC) was also established as a consequence of emphasized importance of cybersecurity at Prague Summit. (NATO, 2002) However the cybersecurity efforts were left to member nations' initiatives and still were not considered as a strategic task of NATO to fulfil.

3.2. 2008 Bucharest Summit

As the member states held responsible to provide security to their own networks and information systems, another significant attack operated as a wakeup call, like it did to European Union's awareness of cybersecurity: 2007 Estonia Attacks

Over the decision of changing the place of a war monument from the Soviet Era, an enormous and well-organized DDoS attack hit Estonian critical infrastructure and kept the country blocked for almost a month.

Following the attacks, as the possible impact that could be achieved through cyberspace with a very little effort has been revealed, in a short period of time the significance of cyber defense was recognized by the Alliance. ("A look at Estonia's", 2009) Hence in the Bucharest Summit held in 2008, emphasizing the changing nature of new types of threats, also the importance of required security measures promised to be taken by the Alliance.

Following the policy and mentioning of enhancing the capabilities with new structures to be established related to cyberspace, Cooperative Cyber Defense Centre of Excellence (CCDCOE) was established in the capital city of Estonia, Tallinn. Besides, also the Cyber Defense Management Authority (CDMA) was established in Brussels following the Bucharest Summit.

As it continues to guide NATO regarding cyber defense issues CCDCOE, were not really related to operational missions, instead established as a research and complementary centre. Following its establishment, a significant effort put forward by the Centre of Excellence, in order to provide *jus in bello* and *jus ad bellum* to cyberspace hence cyberwarfare, the Tallinn Manual was issued in 2013.

While the Manuel draw attention of the media and legal societies even in when it was only a draft (Boyle, 2012) right after its publication, it was accepted as the main authority regarding the applicability of the law of armed conflict for cyberspace, especially western world. (Luukas et al, 2016) 4 years later, CCDCOE published a more comprehensive Manual called Tallinn 2.0.

Finally, as the Alliance held another summit in 2009 in Strasbourg and Kehl for the 60th anniversary of the establishment of NATO, the same topics and effort put forward was emphasized once again. Besides, more work was promised especially those which will be established with international organisations and also third countries. (NATO, 2009)

3.3. 2010 Lisbon Summit

Following the great effort put forward right after the Estonia attacks, focus on defensive enhancement regarding cyber defence continued also in the 2010 Lisbon Summit and the NATO Strategic Concept published in the same year. (Healey & Bochoven, 2012:1)

While in the summit, while uninterrupted access to and integrity of critical systems was emphasized, significantly, cyberspace was mentioned as a new dimension of modern conflicts and hence taken into NATO's doctrine. In this regard, improvements of related capabilities, making NATO Computer Incident Response Capability achieve reaching its fully operational capacity by 2012 and the requirement of cooperation and close coordination with other actors, like the United Nation and the European Union were underlined. (NATO, 2010)

Besides, also in the strategic concept declared in the same year, rapidly increasing complexity,

and sophistication of cyberattacks with also growing numbers once again emphasized within the Security Environment chapter. Importantly, not only the attacks against state systems or networks, but also attacks that are directed to the private sector, transportation and other related critical infrastructure were also mentioned. ("Strategic Concept…" , NATO, 2010)

3.4. 2011 Policy on Cyber Defense

Following the acceptance of cyber defence as a strategic matter and inclusion of it to the strategic concept, especially with also the effects of the cyberattacks that targeted NATO after the operation in Libya, in 2011 NATO extended its first cyber security policy and published a new one that covers more of required concepts.

The second policy on Cyber Defence was issued in 2011. While the drafting was first made in march, it took 2 more months to finalize the document and attached implementation tool, namely the Action Plan, on 8 June 2011.

While the focus of the plan was to protect the integrity and continuity of relevant systems, in order to develop required cyber defence capability, also NATO Defence Planning Process was given as a guidance for the integration of cyber defence into national defence frameworks. To this end, identification of related networks and information systems and bringing all NATO bodies under a centralized cyber defence program to provide sufficient protection and ensure operationality of the Alliance networks, determined as significant once again. (NATO, 2011) As the possibility of a collective response was also mentioned, responsibility and right to take such a decision was given to the North Atlantic Council. (NATO, 2011)

A new scheme named Cyber Defence Governance was drawn which put North Atlantic Council in the first stage and respectively; Defence Policy and Planning Committee in Reinforced Format, NATO CDMB, NATO CIRC

3.5. 2012 Chicago Summit and NCIA

A year later from the second policy, in the Chicago Summit, cyber defence measures were once again taken into consideration. Almost as a tradition, in the declaration of the summit, first, the works and promised progresses of previous summits and policies were emphasized and required effort was mentioned to fulfill the stated goals. (NATO, 2012) In the summit, further cooperation with the European Union, the Council of Europe, the United Nations and the Organization for Security and Co-operation in Europe, was emphasized. (NATO, 2012)

Two months later the Alliance merged its existing command, control and communication(C3) organizations and established the NATO Communications and Information Agency (NCIA). (NATO Communications and Information Agency [NCIA], 2020) Most basically, the responsibilities of this new agency was decided as providing relevant information technologies support to any NATO agencies, headquarters (HQ) and command structures. Which also put NCIRC under the rule of the Agency. However, NCIA is not only responsible for cyberspace related issues but also subjects such as air and missile defence command and control, are also in the extent of the Agency. (NCIA, 2020)

In order to establish sufficient cyber security among the Alliance, in 2013, Multinational Cyber Defence Capability Development (MN CD2) program was initiated by the NCIA with five founding members: Canada, Denmark, the Netherlands, Norway and Romania. While Denmark and Norway left the program afterwards, Finland later participated. Within the program, the role of the NCIA is designed as the coordinating and enabling body with the commitment of achieving goals determined for the program. (NCIA, 2020)

3.6. 2014 Wales Summit

As the Alliance progressed a step further with each summit in the cyberspace area, in order to follow the rapid changing nature of it; in Wales Summit, cyberspace measures were also taken into consideration especially as a part of hybrid warfare. (NATO, 2014)

To this end, cybersecurity based decisions explained in two articles for the first time with the Wales Summit. In these articles, the fundamental duty of the Alliance in this regard is stated as defending the networks that belong to Alliance itself and assisting member states in order to make them provide adequate level of security to their national systems and networks.

Besides, with this summit, while the Alliance

declares the acceptance of the application of international humanitarian law and the UN Charter to cyberspace, it also states the possible use of collective defence clause of the Alliance due to increasing damage capability of the cyberattacks and dependency of modern western societies to integrated networks and information systems. In this regard, the decision whether Article 5 was triggered by an attack would be taken by the North Atlantic Council on a case by case basis.

3.7. 2016 Warsaw Summit and The Cyber Security Pledge

After the huge progress from 2008 to 2014 by the Alliance, in the 2016 Warsaw Summit, a whole new paradigm was accepted by heads of state and government of the member countries. With this new paradigm, the Alliance designed a new role to itself. In that sense, NATO decided to define cyberspace as a domain of possible operations.

To this end, in the summit declaration, while the cyber threats described as a clear challenge to security and prosperity of the Alliance and its members, they are acknowledged as harmful as any threats that can be directed from conventional dimensions. In addition to previously mentioned application of UN Charter and international humanitarian law to cyberspace, with the Warsaw Summit also significance and application of human rights to cyberspace was stated. (NATO, 2016) Besides, in order to achive providing the promised security and enhance cyber defence of the alliance, while the NATO Industry Cyber Partnership defined as an important project; also international cooperation and especially coordination with the European Union once again mentioned. In that sense, the technical agreement established between two organization in the same year was appreciated.

Finally, the Heads of State and Government of the Member Countries defined the 7 areas of efforts, which also includes cyber defence and relatedly information protection. They also issued the Cyber Defence Pledge which, naturally, consists of promises and expectations of member states and the Alliance from them. With the Pledge, while evolving the dangerous nature of cyberspace and acceptance of it as an additional dimension to previous conventional dimensions acknowledged; also the promise of enhancing national capabilities with allocating required resources and commitment to the Enhanced Policy on Cyber Defence, repeated. (NATO, 2018)

3.8. 2018 Brussels Summit and Cyber Operation Centre

Following the decision of considering cyberspace as an addition to conventional dimentions, growing attention paid by NATO to cyber defence also continued in 2018 Brussels Summit. Although the ongoing emphasizing process through summit continues, aggressive behaviour of the Russian Federation, for the first time, expressed within the declaration directly. In addition to this, problematic situation occured due to faced hybrid challenges consist of disinformation campaigns and cyberattacks are also underlined. (NATO, Brussels Summit, 2018)

Besides, also the necessity of more regular exercises including exercises organized related to cyberspace explained. In that case, it is possible to see the changed approach of the Alliance to the cyberspace especially from laissez faire principle to more acknowledged and effort worthy type of dimension.

Besides, another body related to cyber security operations included to the NATO Command Structure, and designed to be established in Belgium, alongside with Joint Force Command Norfolk, Joint Support and Enabling Command, namely; Cyberspace Operations Centre (CyOC). In this regard, Cyberspace Operation Centre is expected to be the backbone of the cyber capability of the Alliance and will serve as the theatre component of the Alliance. (Brent, 2019)

In accordance with its principle, NATO organizations that are operating fully or partially to provide a sufficient level of cyber defence the Alliance and principle educational institutes which are either totally based on cyberspace education or extended their scope in sense of including cyber related issues can be tabled as shown below, in Figure 9.

Educational Institutes	Cybersecurity Organizations
NATO Computer Incidents Response Capability (Mons, Belguin)	
Cyber Operations Centre (Mons, Belgium)	The Cooperative Cyber Defence Centre of Excellence (CCDCOE; Tallinn, Estonia)
Allied Command Operations Task Force Cyber (Mons, Belgium)	NATO Communications and Information System School (Latina, Italy)
Allied Command Transformation (Norfolk, Virginia)	The NATO School (Oberammergau, Germany)
Intelligence and Security Division (Mons, Belgium)	The NATO Defence College (Rome, Italy)
Intelligence Fusion Centre (United Kingdom)	

Figure 9: Cyber Security Organizations and Educational Institutes of the NATO (Ablon et. al, 2019)

3.9. Cyber Defence Exercises

As it has been mentioned several times in different documents, the Alliance pays a significant amount of attention to exercises aiming to strengthen its cybersecurity. In this regard, as there are plenty of exercises taking different aspects of various scenarios of cyberspace, here we will mention relatively more important two of them, namely; Locked Shields and Cyber Coalition.

Since 2007, NATO continues to hold annual cyber defence exercise called Cyber Coalition, which is also described as flagship cyber defence exercise of the Alliance. And the participant number grows by each year. While the exercise gives the chance of testing the skills of cyber defenders in sense of defending the networks and information systems of the Alliance and also their countries, it also trains those participants in order to make it possible to achive further goals.

Besides one of the main goal of the exercise is, naturally, establishing a coordination and enabling cooperation among the participants, by enhancing the ability to protect related part of cyberspace and conduct military operations in it. ("Cyber Coalition", 2018)

To this end, with the addition of academics and representatives of industry, for the first time in 2014, participant numbers reached over six hundred. Following years, as more civilian and expert joins, the number grows over a thousand.

In the exercise occurred in 2019, the procedures with NATO's Cyberspace Operations Centre was also emphasized. As the Lieutenant Commander Robert Buckles, who was the Exercise Director, explains; "*This year we emphasized warfare development through new experimentation, development of new tactics, techniques, and procedures with NATO's Cyberspace Operations Centre (CyOC). And further enhance coordination and collaboration amongst the Alliance within the Cyberspace Domain of Operations.*" ("Exercise Cyber Coalition", 2019) Another important annually organised exercise in order to enhance skills of cyber security experts to enable them defend national IT systems and critical infrastructures in case of a real-time attack is; Locked Shields.

Since 2010, NATO keeps the Locked Shield going in order to enhance its capability and skills of IT personnel of the member nations. In time inclusion of the representatives of industry, the variety of the participants also increased. While

the exercise is basically a cyber war game where a team or a group of teams trying to protect pre-determined systems and networks, another in-game villian team attacks and tries to use the most sophisticated real-time methods in order to keep it as near as possible to real-time scenarios. In this regard, this annual exercise is being described as "the World's largest and most advanced international technical live-fire cyber deterrence exercise" by the Alliance. (Calatayud, 2017)

4. Cooperation Between Two Allies

Following the description and definition of cyberspace related concepts and cybersecurity approaches of both organizations, under this title, a brief background to understand the current position of organizations and their cooperation in cyberspace with further possibilities will be examined.

4.1. Brief Background and Conventional Problems

Although both organizations built upon similar values that can be defined as " Western Values", refer each other as " strategic partners" (Aghniashvili, 2016:68) and shares 22 members; raises concerns of non-European members and also the Alliance in regard to losing the pivotal role of European Security to another relatively new organization and fall into duplication hence make unnecessary effort. Beside the common members, also the mandates of the NATO and European Security and Defence Policy is overlapping largely, in sense of Petersberg Tasks and both comprehends no geographical boundaries (Hofmann, 2019: 45) which sometimes results with simultaneously arranged operations with no formal link.

Following this, special case of non-dual member countries are also creating a problematic situation between two organizations and poses an obstacle for further cooperation, especially in conventional dimensions. In particular, the situation between one of the significant NATO member, Turkey, and a relatively new member of the Union, Southern Cyprus, is being pointed as one of the main impediment that blocks further cooperation of the organizations. (Hofmann, 2019: 45)

In that sense, while Turkey constantly refuse any attempt that includes reach of Southern Cyprus to any NATO assets or resources, especially in sense of intelligence sharing due to security concerns; Southern Cyprus also blocks already problematic position of membership process of Turkey and especially the participation possibility of Turkey to the European Defence Agency, which in sense of preserving status quo should have been granted as a right to Turkey.

4.2. Cooperation in Cyberspace

However, despite the problematic consequences of the establishment of European CSDP and although such political deadlocks still exist between organizations, a new momentum to push cooperation between each other reoccurred in 2016 with a joint declaration issued by the president of the EU Council, the Commission, and the secretary general of the NATO. ("Joint Declaration", 2016)

In fact, it would be more proper to state that the relations in regard to cyberspace between organizations is started with the joint declaration of Warsaw. As there were only a technical agreement that foresees promotion of further cooperation between NCIRC and the CERT-EU.

While there was a clear intention of increasing relations between organizations, especially regarding cybersecurity, for so long, those intentions were not able to go further than just being verbally expressed. In fact, with also the heritage of having different nature than each other where NATO is a political-military international organization, and the EU is parliamentary, economical, and trading based supranational organization; the general approaches adopted by the NATO and the EU are also complementing each other.

In accordance with this, first step of increased cooperation on cybersecurity and defense was forementioned technical agreement which was followed with implemented aspects of the joint declarations. As the technical agreement tried to create a common understanding against the similar challenges that both response teams are struggling with, its framework basically and briefly is consist of information and practices sharing between the NCIRC and CERT-EU. To this end, also participation of EU to Cyber Coalition (Cybersecurity exercise performed by NATO), can be taken as an example of intentions of organizations to have their efforts collaborated.

Following this, joint declaration decisions of 2016 especially stated the necessity of exchanging

concepts of the integration of cyber defense approaches, increasing cooperation in exercises, promoting innovation cooperation in cyber defense research, and finally harmonizing the training requirements and cooperation in trainings. ("Statement", 2016)

Within the period that will be examined hereby, there has been 4 reports regarding the 2016 Joint Declaration;

1. The first report issued on 14 June 2017. Due to comprehensive extent of joint declaration, as it includes several different subjects, according to cybersecurity, main point of report was to intensify cooperation in cyberspace. (NATO, "Progress report on the implementation", 2017)
2. Another report issued briefly after first one on 29 November 2017. (NATO, "Second progress report", 2017) In the report, an important step forward in accordance with goals set to encounter the hybrid threats taken into consideration, establishment of the European Centre of Excellence for countering hybrid threats, in Helsinki. Besides, also the first parallel and coordinated exercise EU PACE17/CMX17 emphasized, which held in September and October of the same year. (NATO, "Common set of new proposals", 2017)
3. The third report (NATO, "Third progress report", 2018) was issued on 31 May 2018. While in the report, proposed 32 further actions on 5 December 2017, in addition to previous 42 of them, accepted in 2016, was taken into consideration; in general the report analyzes the achievements of cooperation and expresses the further possibilities of increasing it.
4. Final report on the progress of the implementation until 2020 regarding to previously mentioned proposals was issued on 17 June 2019. Intensified political dialogue and increasing cooperation were the main points of the cybersecurity aspect of the report. In fact, other subjects such as conventional and hybrids threats were more frequent in the last report.

Beside the 2016 Joint Declaration and 4 reports on it, to increase and accelerate the cooperation process; in 2018 these 2 international organizations have declared second joint declaration stating the intent of further cooperation especially against hybrid and contemporary threats. (NATO, "Joint Declaration ", 2018) However, due to detailed mentioning of cybersecurity in previous reports, the second joint declaration was not necessarily deepened in sense of cyberspace. Instead, cybersecurity was mentioned whenever hybrid threats were taken into consideration.

Indeed, these problematic uneven approaches and nation-based considerations not only pose an obstacle for further cooperation between organizations but also have critical effect within. Nevertheless, while transboundary nature of cybersecurity requires states to have a well international coordination among each other.

5. Common Threats and Possible Future Chances

As a matter of fact, plenty of attacks from a variety of sources including states and non-state actors targeting Europe and North America constantly and increasingly. Especially Russia and China should be taken into consideration with some important examples and their main goals to launch such offensive campaigns.

Besides the milestone attacks like Estonia in 2007 and Georgia in 2008, as expectedly Russian offensive targeting western structures and democracies didn't stop at any point. To this end, while the superiority in cyberspace was defined as one of the essential goals for Russian Federation, in their National Security Strategy, also the confrontation in the worldwide information dimension was emphasized.

A variety of democratic processes can be given as example of targeted processes by Russia, in order to either prevent or promote self-proclaimed ideas about those elections or at least to lower the trust in democratic ways and western values, including; Italian elections in 2018, French elections in 2017, the Brexit referendum, and the most popular among mentioned, the 2016 United States Presidental Election. (France24, 2017)

Another actor in cyberspace and with its emerging role in conventional dimentions also, is the People's Republic of China (PRC). Following the military modernization process, PRC also paid an important level of attention to enhance its cyber capacity, especially to have an offensive capacity in cyberspace and to use it to capture especially economic classified information through unauthorised ways and to cyberespionage. Unlike Russia, commercial gain is more preferred by PRC in that sense. To this end, infiltration to 5 US companies, in 2014, by Chinese hackers who eventually found out was People's Liberation Army (PLA) officers and charged by US Justice Department, shows this

intention of PRC clearly. (US District Court, 2014)

To this end, 3 basic suggestions can be stated to increase the cooperation between organizations;

5.1. To achieve having a joint response mechanism, the most important step forward is to establish an Interorganizational Cyber Threat Information Centre.
5.2. Following this establishment of a joint computer response team that will have coordinated staff from NATO CIRC as well as CERT-EU would be an important step.
5.3. A following step would be the creation of a joint program to fund the computer response teams of the organizations, national computer response teams, the joint response team. As a matter of fact, while preventive and deterring actions needs a financial support; the creation of such fund, would be more useful if initiated with previous steps.

Conclusion

Since the creation of the first network in the second half of the 20th century, emerging network and information system technology rapidly dominated almost every aspect of daily life, politics, society and economics. As the internet evaluate from Web 1.0 to Internet of Things, through time, cyberspace developed its own rules and concepts. New set of tools and dimension also transformed the conventional ones and constructed new concepts like; cyber defense, cyber espionage et. al.

Transforming nature of emerging technologies, expectedly effected the international relations and the most important turning point of cyberspace has been the first highly organized and intensified DDoS attacks targeting Estonia in 2007. As a matter of fact, Estonia Attacks not only served as a national wakeup call but also triggered the attention of the European Union which Estonia was participated with 2004 enlargement and the NATO, participated in 2004 as well.

In order to preserve its continuing provision of security and stability to their member while the European Union accelerated its process to build upon previous, less intensified attempts, with a directive on identification and designation of its critical infrastructure, in 2008 (EC, 2008); also the NATO initiated a serious process of progress starting with the establishment of a Cooperative Cyber Centre of Excellence based in Tallinn at the first summit after the attack, in 2008 as well.

In fact, until 2016 two organization have followed formally separated ways, but nevertheless due to their different nature; the general approaches adopted by these two organizations are occurred as complementary work of each other. However, such cooperation still needs a more enhanced and sincere cooperation. The necessity occurs due the requirement of the cyberspace of a more comprehensive understanding that passes the border-based ideas.

Although the organizations have conventional problems including but not limited to duplication and non-dual membership; these doesn't prevent both actors to construct more cooperative future in cyberspace. Nevertheless, joint declarations and cooperative efforts still doesn't seem deep enough to create a spill-over effect over abovementioned problems.

While it would not be logical for the European Union to try constructing a separated cyber security, reciprocatively it would also be fatal error for the North Atlantic Treaty Organization to separate its efforts from cyber security progress of the previous actor. Hence, there is more chances to take advantage of, by both organizations and sincere approach to each other would help to have a more secure future for both actors.

Bibliography

A look at Estonia's cyberattack in 2007 (2009, July 8) CBS News, retrieved from http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/ .

Ablon L., Binnendijk A. & et. al. (2019), Operationalizing Cyberspace as a Military Domain Lessons for NATO. Rand Corporation.

Aghniashvili, T. (2016) Towards More Effective Cooperation? The Role of States in Shaping NATO-EU Interaction and Cooperation. Connections, 15(4).

Boyle A. (2012, Sep 24) International law takes on cyber: significant challenges ahead, The Hill, retrieved from https://thehill.com/blogs/congress-blog/technology/251279-international-law-takes-on-cyber-significant-challengs-ahead.

Brent L. (2019) NATO's Role in Cyberspace. The Three Swords Magazine, 34, retrieved from http://www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/NATOCyberspace.pdf.

Catalyud J. M. (2017, Jun 18) Locked Shields: The world's largest cyber-war game, Al Jazeera, retrieved from https://www.aljazeera.com/indepth/features/2017/05/locked-shields-world-largest-cyber-war-game-170527102554714.html (09.06.2020).

Chivvis C. S. (2017), Understanding Russian "Hybrid Warfare" And What Can Be Done About it, retrieved from https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf .

Cornish P., Livingstone D., Clemente D., & Yorke C. (2010). On Cyber Warfare. Chatham House.

Council of the European Union, European Parliament. (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the committee of the Regions of 7 February 2013 " Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" JOIN(2013) 1 final, communication paper.

Council of the European Union. (1992), Council Decision of 31 March 1992 " in the field of security of information systems" (92/242/EC).

Council of the European Union. (2011), Adoption of Council conclusions of " Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP)" 10299/11, conclusion paper, retrieved from http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf .

European Commission, European Parliament. (2000), Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions of 21 January 2001 " Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime", COM (2000) 890, communication paper

European Commission, European Parliament. (2011), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions of 31 Mart 2011 " on critical infrastructure protection, Achievements and next steps: towards global cyber-security" COM(2011) 163 final, communication paper.

European Commission. (2006), Communication from the Commission of 12 December 2006 " on a European Programme for Critical Infrastructure Protection " COM(2006) 786 final.

European Commission. (2013), Commission Staff Working Document Impact Assessment of 19 September Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council " On Enisa, the ' EU Cybersecurity Agency' and repealing Regulation (EU) 526/2013, working document.

European Commission. (2013), Policy on Critical Information Infrastructure Protection (CIIP), retrieved from https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip.

European Commission. (2017), Commission Staff Working Document Impact Assessment of 19 September Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Information and Communication Technology Cybersecurity Certification: Cybersecurity Act" SWD/2017/0500 final, 2017/0225 (COD), communication paper.

European Council. (2008), Council Directive of 8 December 2008 " on identification and designation of European critical infrastructures and the assesment of the need to improve their protection" (2008/114/EC).

European Network and Information Security Agency. (2017), Overview of Cybersecurity and Related Terminology Version-1, retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology.

European Parliament, Council of the European Union. (1995), Directive of the European Parliament and of the Council of 24 October 1995 " on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (95/46/EC).

European Parliament, Council of the European Union. (2002), Directive of the European Parliament and of the Council of 12 July 2002 " concerning the processing of personal data and the protection of privacy in the electronic communications sector" or Directive on privacy and electronic communications 2002/58/ EC, directive paper.

European Parliament, Council of the European Union. (2004), Regulation of the European Parliament and of the Council of 10 March 2004 " establishing the European Network and Information Security Agency" (EC) No 460/2004

European Parliament, Council of the European Union. (2008), Regulation of the European Parliament and of the Council of 24 September 2008 " amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration" (EC) No 1007/2008

European Parliament, Council of the European Union. (2013), Regulation of the European Parliament and of the Council of 21 May 2013 " concerning the European Union Agency for Network and Information Security and repealing Regulation (EC) No 460/2004" (EU) No 526/2013.

European Parliament, Council of the European Union. (2016), Directive of the European Parliament and of the Council of 6 July 2016 "concerning measures for a high common level of security of network and information systems across the Union" (EU) 2016/1148.

European Parliament, Council of the European Union. (2019), Regulation of the European Parliament and of the Council of 17 April 2019 " on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) NO 526/2013: Cybersecurity Act" (EU) 2019/881.

European Parliament. (2012), European Parliament resolution of 12 June 2012 " on critical information infrastructure protection, achievements and next steps: towards global cyber-security" 2011/2284 (INI), retrieved from https://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167 (24.05.2020).

France24. (2017), Cyber experts '99% sure' Russian hackers are targeting Macron, retrieved from https://www.france24.com/en/20170426-france-macron-cyber-security-russia-presidential-campaign

Gary S., Jessica E., & Katherine T. P. (2009). The Internet- Illustrated. Boston: Course Technology Cengage Learning.

Healey J., & Bochoven L. (2012), NATO's Cyber Capabilities: Yesterday, Today, Tomorrow, retrieved from https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf .

Hofmann S. C. (2009), Overlapping Institutions in the Realm of International Security The Case of NATO and ESDP. Perspectives on Politics, 7(1).

Ilves L. K., Evans T. J., Cilluffo F. J., & Nadeau A. A. (2016), European Union and NATO Global Cybersecurity Challenges: A Way Forward, PRISM, 6(2), retreived from https://cco.ndu.edu/News/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/.

James A. Green (Ed.). (2015), Cyber Warfare: A multidisciplinary analysis. New York: Routledge.

Libicki M. C. (2007). Conquest in Cyberspace. RAND Corporation.

Libicki M. C. (2009). Cyberdeterrence and Cyberwar. RAND Corporation.

Matishak M. (18 July 2018) What we know about Russia's election hacking, Politico, retrieved from https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087.

North Atlantic Treaty Organization Communication and Information Agency. (2020), About Us, retrieved from https://www.ncia.nato.int/about-us.html.

North Atlantic Treaty Organization Communication and Information Agency. (2020), What We Do, retrieved from https://www.ncia.nato.int/what-we-do.html.

North Atlantic Treaty Organization. (2002), Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic, retrieved from https://www.nato.int/cps/en/natohq/official_texts_19552.htm?selectedLocale=en.

North Atlantic Treaty Organization. (2002), Prague Summit Declaration, retrieved from https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

North Atlantic Treaty Organization. (2009), Strasbourg / Kehl Summit Declaration, retrieved from https://www.nato.int/cps/en/natohq/news_52837.htm.

North Atlantic Treaty Organization. (2010), Lisbon Summit Declaration, retrieved from https://www.nato.int/cps/en/natohq/official_texts_68828.htm.

North Atlantic Treaty Organization. (2010), Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.

North Atlantic Treaty Organization. (2011), The NATO Policy on Cyber Defence.

North Atlantic Treaty Organization. (2012), Chicago Summit Declaration, declaration.

North Atlantic Treaty Organization. (2014), Wales Summit Declaration.

North Atlantic Treaty Organization. (2016), Joint Declaration by the president of the European Council, the president of the European Commission, and the secretary general of the North Atlantic Treaty Organization.

North Atlantic Treaty Organization. (2016), Progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016.

North Atlantic Treaty Organization. (2016), Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, retrieved from https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

North Atlantic Treaty Organization. (2016), Warsaw Summit Declaration.

North Atlantic Treaty Organization. (2017), Common set of new proposals on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, retrieved from https://www.nato.int/cps/en/natohq/official_texts_149522.htm?selectedLocale=en.

North Atlantic Treaty Organization. (2017), Second progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016, 29 November 2017.

North Atlantic Treaty Organization. (2018), Cyber Coalition Helps Prepare NATO For Today's Threats, https://shape.nato.int/news-archive/2018/cyber-coalition.

North Atlantic Treaty Organization. (2018), Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, retrieved from https://www.nato.int/cps/en/natohq/official_texts_156626.htm.

North Atlantic Treaty Organization. (2018), The Cyber Defence Pledge, retrieved from https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en.

North Atlantic Treaty Organization. (2018), Third progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017.

North Atlantic Treaty Organization. (2019), Exercise Cyber Coalition 2019 Concludes in Estonia, retrieved from https://shape.nato.int/news-archive/2019/exercise-cyber-coalition-2019-concludes-in-estonia.

Scott J. (2017), Strategic Cyber Deterrence: The Active Cyber Defence Option. New York: Rowman & Littlefield.

Sweeney J., Holsoe J. & Vulliamy E., (1999, Oct 17) Nato bombed Chinese deliberately, The Guardian, retrieved from https://www.theguardian.com/world/1999/oct/17/balkans.

Szentgali G. (2013) The NATO Policy on Cyber Defence: The Road So Far. AARMS 12(1).

The Computer Emergency Response Team EU. (2015), New Headquarters for CERT-EU, retrieved from https://ec.europa.eu/newsroom/informatics/item-detail.cfm?item_id=26069.

The Computer Emergency Response Team EU. (2020), About Us, retrieved from https://cert.europa.eu/cert/plainedition/en/cert_about.html.

The North Atlantic Treaty Organization. (2018), Brussels Summit Declaration, 11-12 July 2018, PR/CP (2018)074.

US District Court. (2014), Indictment, Criminal No. 14-118.