Cybersecurity in Europe: a take on NATO Article 5 in the light of the Trump-Russia case
Table of Contents

Abstract ....................................................................................................................... 3
1. Introduction ............................................................................................................. 4
   1.1. Research questions .......................................................................................... 5
   1.2. Hypothesis ....................................................................................................... 6
   1.3. Research design and methodology ................................................................. 6
2. What is cybersecurity? ............................................................................................ 12
3. Mapping out cybersecurity threats ...................................................................... 15
   3.1. Threats concerning our personal space and private business ...................... 15
   3.2. Threats apropos of the public sphere, government-run systems and national security .... 18
   3.3. Security versus privacy ................................................................................... 20
4. NATO as a centerpiece of European security and Article 5 ............................. 23
5. Cybersecurity in NATO ....................................................................................... 28
6. International legal background: invocation of Article 5 by a cyber-attack .......... 38
7. Russia’s influence campaign targeting the 2016 US presidential election and the Trump-Russia affair ................................................................. 43
8. Implications of the Trump-Russia case for NATO Article 5 ......................... 50
9. Conclusion ............................................................................................................. 51
Bibliography ............................................................................................................. 54
Abstract

This research paper tries to answer the question whether the hacking and other cyber intrusions and meddling with the USA presidential race in 2016 by supposedly Russian hackers brings NATO closer to creating a stable legal environment for cases of cyber-attacks, namely making cyber-attacks a trigger like any armed attack for invocation of Article 5 (collective defense obligation). The paper looks at the major cyber threats and NATO’s capabilities to counter them and well as the details of the Trump-Russia affair and its effect on the process of paradigm change with regards to collective defense to counter cyber-attacks. The aim of this paper is to present the most up to date information on the issue and warn about the problems (and benefits) of a broad and unstable legal environment that lacks specifics conditions and explicit thresholds.
1. Introduction

It is imperative to keep theory, legal concepts and practices up to date in the field of politics, international relations and diplomacy in order to make the best possible decisions and extract maximum benefit from the possibilities – even more so in the 21st century when the world is speeding up and changes occur what often feels overnight. The cyber domain is one of those novel areas of international relations where the tendencies of the new millennium are manifested the most: power is dispersed and decentralized, borders are blurred, actors are diverse ranging from state authorities to the average commoner with a smartphone, and the environment is ever changing. This research paper has been written with the mission to summarize the most important and novel information on developments in cyberspace and related infrastructure and supplement it with the most recent issues and subjects of discussion.

The topic is so broad it is a must to set boundaries to this research to make results accurate and meaningful. One of the most targeted and broadly discussed areas nowadays is Europe and the security challenges it faces. One of the aspects of said security concerns is that of the cyber domain. The emergence of world wide networks and information systems is relatively recent therefore, relevant authorities have started to create policies with regards to cyber incidents only some three decades ago. Before that ICT has been relatively unregulated and a true free space from state intervention. However, times have changed. Today many of the state’s functions are performed through the cyberspace, regular users are in need of protection from cybercriminals, and there is a looming fear of cyberwar as part of the hybrid warfare strategy which prompts defense organizations to bring this question at the forefront of their agenda.

Understandably, the examination of the legal side of the issue has also been popular with academia. One thing is certain: there is no universal binding document warranting an international law or norm that explicitly states the position of cyber-attacks in the so-called law of war. This grey area is exploited by aggressors and used to terrorize their victims be it states or private individuals. In this paper I am going to describe the pre-existing legal environment that the newly created laws and norms have to be embedded into and also some other sources that serve as guidelines for responding to cyber incidents.

We live in the era of the society of states where the use of force as a means of resolving contentious issues is outlawed. As a consequence, most states belong to collective defense organizations to channel their military might. Without a doubt currently the leading such organization in Europe is NATO. Collective defense is enshrined in Article 5 of its founding
Charter and with the emergence of regular cyber threats to its Members’ security it inevitably comes under scrutiny. The question whether cyber-attacks can be or should be regarded as an armed attack just like nuclear or conventional attacks has become pressing. Although the NATO is gradually moving towards the recognition of cyber-attacks as a legitimate reason to invoke Article 5, the legal background to cement this view is yet to be created. Possibly the case of the meddling of Russian hackers with the 2016 USA presidential elections will be the incident to push this process towards its culmination. Although there have been previous cyber-attacks by Russian hackers in the past this case might be different. Not only did it occur in the heart of the most prominent member state of the NATO but it also meant an intrusion into the most sacred Western principle of liberal democracy.

1.1. Research questions

In the following section I will briefly introduce the research design used for this paper.

The main question I am looking at in this research is whether the intrusion and other related incidents in the cyberspace of candidates of the 2016 USA presidential election by Russian hackers (1) have happened (2) influenced the election outcome (3) has any implications for the use of Article 5 of NATO in case of cyber incidents.

As the introduction suggests this research paper retains its value from bringing up to date the existing academic literature on the incidents that have contributed to the NATO technical, political and legal cyber preparedness by examining the potential effects of the Trump-Russia affair on invocation of Article 5 in case of cyber-attacks. Furthermore, the relevance of cyber incidents and responses to those is especially high due to the ongoing Ukraine crisis as it is one of those conflicts where hybrid warfare has been employed with the cyber component as one of the major legs of the operations. As the political climate is getting ever colder sometimes the “Second Cold War” phrase comes up when referring to Europe. Russia has displayed aggressive and uncooperative attitudes with regards to respect of international rules and norms when it annexed Crimea and supported and continues to support ethnic Russian separatists in Ukraine. The NATO, following the expansion in its membership, is now once more experiences Russian aggression close to its Easter European borders. Russia has shown readiness to use cyber warfare in several cases and is likely to do so in the future. Therefore, it is imperative to have a solid legal background with regards to invocation of Article 5 to avoid confusion and costly delays if a NATO member state or the NATO’s own
infrastructure is ever under a cyber-attack. This is partly the reason why this research question is so important to ensure stability in Europe and in the broader Transatlantic area.

1.2. Hypothesis

The hypothesis I am working with in this paper is based on two assumptions. The first one is that in an international organization with a broad membership like NATO it is always difficult to make changes to the existing rules and procedures as it is difficult to please all stakeholders. On the other hand, because the intervention into the 2016 USA presidential elections was a blow to the political independence of NATO’s leading member state, the United States it should be more of an incentive for change than Russia’s previous cyber-attacks (Estonia, Georgia and Ukraine). The hypothesis therefore is that there is an above average effect on the legislative preparedness of NATO to cyber-attacks (Article 5 invocation) by the Russian hacking and leaking of emails of the Democratic National Committee and the Hillary Campaign, however this effect will be delayed and gradual just as before.

1.3. Research design and methodology

For this particular research I will use the so called “engineering research” which is an empirical applied method of political research (Shively 2017, pp.4-7). It aims at analysis of real-world problems instead or normative or theory-based methods. The main goal is impact evaluation. I will attempt to make descriptive inference (answering the question “how”) using empirical data presented in legal documents and verbal statements of relevant politicians and scholars.

In the following chapters I am going to elaborate on the current stance of cybersecurity touching upon both the role of the cyber domain in the security aspect of international relations and the main cyber threats that pose danger to it. After that I will describe the NATO and its role as a centerpiece of European security as well as the aforementioned Article 5. Thereafter, I will provide s short overview of the cybersecurity architecture of NATO and the current standpoint of the international community on the application of Article 5 in cases of cyberattacks. Consequently, I will outline the Trump-Russia case of 2016 and finally deliberate on the implications of the Trump case for Article 5 and the road ahead of NATO. Lastly, I will shortly summarize my findings in a concluding chapter.
The methodology employed rests on primarily constructivist assumptions. As previously outlined in my hypothesis rather than rationally assessing the real dangers of lacking a solid legal background regarding the invocation of Article 5 in case of cyberattacks, NATO decision makers let each and every attack be deliberated upon in a political context on a case by case basis. Due to NATO’s organizational structure, group dynamics fog the presented and well-known facts and allow other - budgetary, nationalistic and normative – considerations to slow down decision making. Therefore, I found it best not to use either the realist or liberalist approach both being rationalistic and mainly concerned with states as actors. Constructivism on the other hand, carries in itself the freedoms of taking into account various actors and diverse causal relationships and therefore, perfectly suits this research design.

In the following section I am briefly going to summarize those pieces of academic literature which beyond specific information or data have provided me with general inspiration and guidance on the topics of cybersecurity in NATO, history of cyber-attacks and confrontations, and the legal background of invocation of Article 5.

Sergeii Karashov describes in his publication ‘Cyberattacks as “Armed Attacks” on the Objects of Critical Infrastructure in light Article 5 of NATO Treaty’ the lack of cybersecurity legislation in Europe, specifically NATO. At the same time, he outlines a few alternatives such as national cyber strategies and guidelines presented by the Tallinn Center of Excellence which is accredited by NATO. The author examines cyberthreats from the viewpoint of attacks against Critical Infrastructure (CI) and Critical Information Infrastructure (CII) and brings up the examples of attacks of Russian hackers against Estonia in 2007, similarly of Russian hackers in Ukraine in 2014 and the Stuxnet case (a malicious software most probably developed by a joint effort of the USA and Israel to destroy Iranian nuclear infrastructure) in 2010.

Equally important, Jamie Shea’s essay is titled ‘Why does NATO’s new Strategic Concept matter?’ which makes for a self-explanatory title. Jamie has written about the four challenges that prompted NATO to revise its Strategic Concept. These are emerging security challenges (WMDs, terrorism, cyberthreats), a bad experience with the costly (financial, engagement duration and manpower-wise) Afghanistan operation, a need to increase connectivity (to private sector, other non-NATO partners among them international organizations, and between the NATO member states national capabilities) to successfully face the new threats and improve communication with smaller members states to reassure them about their position. Dr. Shea further describes that NATO is shifting its focus from protection of territorial borders to new challenges like missile defense, proliferation of WMDs, cyber threats, energy security, and ensuring the undisturbed operation of global communications,
transport and trade. Shea is the Deputy Assistant Secretary General at the Emerging Security Challenges Division of NATO, so he is one of the best sources if not the best when it comes to credible information regarding the future of NATO.

In like manner, Lieutenant Colonel Charles L. Matallana of the United States Army in his 2017 report titled ‘Maintaining NATO’s Relevance in the 21st Century’ describes how NATO’s perception of its main threat factors evolved over the years. From the traditional NATO vs. Warsaw Pact divide and nuclear and conventional deterrence, to the post-Cold War expansion and non-state actors and separatism, up to the current situation which is characterized by three main challenges. These are: renewed Russian aggression, cyber threats and reluctance of member states to commit to equal burden sharing. Matallana recommends reliance on credible deterrence by (1) encouraging European NATO member states to honor their obligations regarding defense spending representing 2% of their GDP, (2) invest more in conventional landpower capabilities AND cyber capabilities to support them (3) and thus counter the Russian threat to the Eastern European allies. Only this way – advocates Matallana – can NATO stay relevant and successful in its operation.

Additionally, Jason Healey, director, and Klara Tothova Jordan, assistant director of the Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security at the Atlantic Council compiled an issue brief for the Atlantic Council’s Smarter Alliance Initiative in 2014 titled ‘NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow’. They describe the history of NATO’s cyber capabilities and policy from the 1999 Kosovo intervention cyber-attacks by Serbian hackers and at the same time by Chinese and Russian hackers in retaliation of (accidental?) bombing of their embassies up to the most recent conflict with cyber threat implications for the NATO in 2014, the Ukrainian crisis. They also evaluate the 2008 official NATO cyber defense policy and its updated version in 2011. Furthermore, they elaborate on the strength and weaknesses of the Alliance’s cyber capabilities. Lastly, they recommend this paper in the attention of NATO policy makers that were meeting not long after the release of the brief in Wales.

In the same fashion, Szentgáli Gergely in his 2013 publication titled ‘The NATO Policy on Cyber Defence: The Road so Far’ gives an in-depth explanation of the development of NATO’s cyber infrastructure (bodies, initiatives, funding) while providing an excellent historical background as an explanation to the “why” and “when” questions. In the end, the author outlines recommendations with regards to the future development of the Alliance’s cyber capabilities, namely: investing into making NATO’s IT systems the most up to date and competitive, developing offensive capabilities to ensure deterrence, increasing cooperation
especially with the EU and the private sectors, conducting regular cyber exercises, and putting the cyber question in focus in general when it comes to strategic planning in the NATO. This piece is especially useful as it is very concise and to the point.

Comparatively, Carla Spiegel in her MA thesis ‘Securing Cyberspace: NATO’s Cyber Defence Policy as a Security Dispositive’ of 2017 takes a normative approach to the legal recognition of cyber threats as acts of armed attack. In the beginning of her research paper the author conceptualizes “dispositive” as a concept by Foucault as cognitive notion referring to the way NATO perceives cyber threats and how that affects the actual cyber environment. The author details the historic background, the triggers that led to the development of NATO’s cyber capabilities in their present state as well as analyzes various implication of the Alliance’s cyber policy. Firstly, the author correctly describes that NATO decision makers can make political decisions about cyber threats and responses without a solid legal background. Next, an evaluation of technical capabilities and shortcomings is highlighted. Consequently, the author details the political thinking behind the strategic conceptualization of cyber threats as part of information and hybrid warfare. Moreover, the role of civil society is illuminated. Lastly, the main point of the research paper is the effect of the NATO’s cyber security “dispositive” on the real-world: the normalization of cyber-attacks in interstate conflicts as well the inherent encroachment of the state on the freedom of the Internet and online private life of their citizens. Additionally, the author draws attention to the difference between the dispositives of NATO and Russia with regards to cyber security and quotes this as a reason for the paralyzed progress of creation of international cyber warfare norms and rules in the UN.

Another issue brief for the Atlantic Council by the Brent Scowcroft Center’s Transatlantic Security Initiative titled ‘Cyber, Extended Deterrence by Franklin D. Kramer, Robert J. Butler, and Catherine Lotrionte offers recommendations to allow the NATO to use its might for deterrence purposes in the cyber domain. The main recommendations of this very technical and innovative brief include: developing warfighting cyber capabilities, creation of “cyber framework nations” (mainly the USA) that help smaller and weaker member states to catch up to the more advanced states, establishment of partnerships on the national level with the the private operators of electric grids and communication services, and lastly updating and making NATO’s cyber confrontations doctrine more specific so that it can be used immediately in case of necessity.

By the same token, Luukas K. Ilves, Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau in their essay ‘European Union and NATO Global Cybersecurity Challenges: A Way Forward’ detail the cyber security related capabilities of Europe both in the framework of the
NATO and the EU and make recommendation with regards to future policies advising increased cooperation of the two organizations. The presence of cyber security legislation in the EU is mention alongside with the lack of the same in NATO. The authors make it a point that a cybersecurity failure on the long run signals state failure in general as cybersecurity is an unavoidable part of warfare now along with kinetic warfare, furthermore it is interwoven with economic performance and the privacy of citizens. The authors made excellent political and technical recommendations due to their high level of expertise in the field.¹

Furthermore, in Z’hra M. Ghavam’s 2016 thesis ‘NATO’S Preparedness for Cyberwar’ for the Naval Postgraduate School Monterey the author uses a novel method to assess NATO’s preparedness for countering cyber threats which the author considers both inevitable and of distinguished importance. A scheme of evaluating NATO’s cyber strategy, cyber cooperation, decision making, political will, crisis management, defense spending, and defense policy prioritization is created and rated on a range from 1 to 3 (not sufficiently, sufficiently but less then optimally and optimally prepared). To accomplish the rating the author uses qualitative analysis of policy papers, journal articles, the North Atlantic Treaty, defense reports, public poll surveys, and case studies. The author concludes that NATO is moderately prepared for a cyber-attack against any of its member states due to the need of improvement in the key areas of decision making, public support, crisis management, defense spending, and defense policies. Recommendations follow. This thesis both in its structure and content served as one of the most important influences over my own work in this research paper due to its perceived excellence.

Moreover, Roger André Tosbotn’s thesis paper ‘NATO and Cyber Security: Critical Junctures as Catalysts for Change’ uses a constructivist approach to outline the change in NATO’s perception of cyber threats in the domain of security. The analysis is performed by looking at NATO documents from 2002 to 2016. The importance of this work is that it reminds us that we, human creatures, decision makers in the NATO and the “other side” (adversary) are not rational even if we strive to be, and that it is imperative to know the limits and the subjectivity of our thinking in order to make the best decisions to ensure peace and stability. This piece inspired me to take the constructivist approach in my thesis.

¹ Luukas Ilves is Counselor for Digital Affairs at the Permanent Representation of Estonia to the EU, Timothy Evans is Senior Advisor on Cyber Strategy and Policy at Johns Hopkins University Applied Physics Laboratory in Arlington, Virginia, Frank Cilluffo is the Director of the George Washington University’s Center for Cyber and Homeland Security, while Alec Nadeau is a Presidential Administrative Fellow at the George Washington University’s Center for Cyber and Homeland Security.
Next, a take on European cybersecurity from the perspective of complementarity is illustrated by Piret Pernik’s excellent piece ‘Improving Cyber Security: NATO and the EU’ by Piret Pernik. Pernik highlights the fact that these two organization have overlapping memberships to a great degree therefore spending on cybersecurity in both directions would be extremely straining on the Member States’ budgets. Furthermore, as outlined in this paper, the two organization have different strengths and weaknesses making them great complementors of each other. NATO primarily focuses on security and defense while the EU deals with broader and non-military aspects of cybersecurity. As examples for the latter among others Internet freedom and governance, online rights and data protection, and internal security are mentioned by the author. Consequently, Pernik gives specific recommendations as to how to effectively improve cooperation between the EU and NATO in the field of cybersecurity.

Following the overview of some of the most important pieces of literature, in the next chapter I describe the importance of the cyber domain in our life, in maintaining its security as well as I outline the most relevant threats to cybersecurity in Europe.
2. What is cybersecurity?

It is an aspect of security, related to the cyber world that is becoming increasingly important as our lives get increasingly interwoven with the cyberspace. Computers and networks that connect them create opportunities never seen before. As these devices become more complex and networks increasingly extensive, as government institutions, companies and private individuals use them for increasingly diverse tasks and more frequently the importance of securing the cyberspace also grows. ICT (information and communication technology) is one of the youngest but most profitable sectors of any economy (being on par with ages old sectors like military, oil, financial, and the pharmaceutical sector), and is also considered as one of the key strategic industries both from a security and economic perspectives.

Cybersecurity risks pose a new type of challenge because of their novel nature and great variety of actors. The cyberspace is a mostly virtual location (apart from the servers), relatively unregulated (even unregulatable), extremely low-cost in terms of access (comparatively to other aspects of national and personal security like nuclear security with equipment being many times more expensive than that of a computer and internet access) and hugely pervasive (taking over many functions in our lives or creating previously non-existing ones). Due to these factors it is a very attractive target of a diverse range of actors – for purposes legal and illegal. Governments introduce computer technology and the cyberspace dimension to an increasing number of state functions, even shifting some into the cyberspace entirely. Examples of such functions are – just to list a few - administration of taxation, electoral campaigns, management of public healthcare (in countries with an extensive welfare state where providing health is a state function and being healthy is a human right) or ensuring dispersion of crucial information (early warning system in case of natural disasters, information about state policies).

Furthermore, cyberspace spurred the appearance of a whole new industry providing access to and allowing use of various functions of cyberspace, and a proliferation of new jobs connected to the management of cyberspace related aspects in existing companies. Lastly, on the individual level, many of us have created a second life for ourselves with an alternative “us”, an avatar on social media, and many activities are now performed utilizing the cyberspace (most commonly entertainment but, as mentioned previously, for some even employment and intellectual life). Regulation of the latter two is also the task of the state. However, who regulates the state’s cyber policy? Certainly, the citizens do, even if indirectly, through the elections. It can be observed that in states where democracy is illiberal or non-existent (Russia, China, North Korea) cyber aggression against their targets is more likely. In reverse logic,
considering the Stuxnet case (a worm developed by the US and Israel to damage and destroy equipment in Iranian nuclear facilities), it would be interesting to inspect those political-administrative layers where democracy couldn’t reach, the “deep-state” which have allowed the creation and use of such a cyber weapon. In case of liberal democracies, on the other hand, with dispersion and transition of state authority and weakening of its monopoly of power in the globalized world system there is a need for involvement of international cooperation (many times in its institutionalized form, as international organizations) to effectively fulfill all these functions of oversight and regulation.

The other side of cybersecurity is prevention and elimination of cyberthreats (accidental occurrences and criminal activity). These activities should also be undertaken with participation of all the actors listed above and even with nonlinear cooperation between these levels (e.g. individuals following regulation created on the level of supranational institutions).

Moreover, we can take a look at cybersecurity from another perspective. Security definitely correlates with economic welfare. Rather than one causing the other, I would argue they have a mutually beneficial relationship. On one hand, the richest countries are those that have the biggest share in the ICT sector and a secure and regulated (not equivalent of censored) cyber environment. On the other hand, if these countries want to keep their ICT industry flourishing and under control, they need to provide a relatively safe and constant environment to preserve investment and consumption levels related to this sector high (evidently states are aware of this as it can be concluded from their policies and dominant political discourse). If we try to compile the list of “network industries” it will become apparent how extensive the range of industries based on or related to the cyberspace is. First and foremost, if we look at the bottom of the production chain, we find the hardware industry. Manufacturing hardware (providing natural resources as production material, assembling, actual production of components, creating blueprints and designing the product, marketing and determining the general direction of the company) has helped many countries to get out of poverty. These countries are often referred to as “economic miracles”, “Asian Tigers” and so forth representing the quick pace and significant scale of their economic growth. Other sectors involve the software industry (from social media and web programming to software computing ICBMs), telecommunications services, broadcasting, information reproduction (Internet as an online library), banking and money (especially with the recent surge of digital currencies and the blockchain technology), transport, entertainment and social interaction, as well as functions like international time coordination.
Despite being a peculiar dimension of security, cybersecurity providers are faced with the same dilemma as in the case of “traditional” security: security and freedom/privacy move on opposite axes. The more one tries to increase security the more freedom has to be taken away from the protected, the more governments try to regulate cyberspace and catch criminals the more they will invade their citizens’ privacy. This central theme serves as a baseline for normative discourse on cybersecurity.

If one would decide to attempt analyzing cybersecurity, the level of analysis could be transnational, national and individual. However, as the field of International Relations is primarily concerned with states and the interaction of those, I have chosen the interstate/international sphere as my level of analysis, and NATO as my unit of analysis. NATO is a peculiar creation, both intergovernmental and transnational: common capabilities and missions coexist with the task of merely providing a platform for cooperation/coordination inducing discussion regarding national policies. In this study, my aim will be to discover the current regulation of cybersecurity in Europe, mainly as an aspect of security, collectively defended through the NATO-WEU-EU triangle.

The most important question hereby is, whether the collective defense clause (Article 5) is activated by a cyberattack, and if yes what should be the scale or scope of such an attack. To answer this question we have to conceptualize cybersecurity and cyberthreats. In the next chapter I will briefly outline the most important threats to cybersecurity. It is essential to explore this as cyberthreats and the scale of the damage inflicted by them will be a decisive factor in determining whether cyberattacks can be considered on par with “armed attacks” (justification for collective defense in the NATO treaty) or attacks that endanger a country’s territorial integrity and political independence (justification for collective defense in the UN charter).
3. Mapping out cybersecurity threats

As outlined above it is super important in today’s world to counter cybersecurity threats to guarantee or at least maximize personal, professional and national safety in general because our lives have become so interwoven with the cyber world. In order to fight these threats in a comprehensive fashion, first it is necessary to explore which are the most prominent ones.

However, first I would like to define the terms cyber incident, cyber-attack and cyber war to avoid any confusion. Cyber incidents are defined as “non-violent cyber operations that seek to obtain, manipulate, or exploit information” (Ghavaml, 2016, p. 22). These can be with the purpose of espionage or any other form of exploitation. Cyber-attacks are also considered to be part of cyber incidents by Ghavaml. Cyber war is a conflict between states or non-state actors that result in “damage, destruction, or death” (Russell, 2014, p. 8).

Although there are countless alternative ways to group them, in this research cybersecurity threats are categorized based on the target of a digital attack or the subject of a cyberspace related liability.

3.1. Threats concerning our personal space and private business

This section outlines the main threats that can endanger any individual in their private life, working environment or other professional activity and business entities like private and semi-state-owned companies.

One of the main threats is ransomware. It is a type of software that encrypts files on any infected device making them unavailable to the user. To decrypt the files the user is demanded to pay a certain amount of money, the ransom. However, even if the user pays most of the time hackers will not bother unlocking the files making this a double scam. One way to prevent having to pay the ransom if one’s device is infected is to always have a backup of the most important files if not all files. It is also possible in certain cases to regain access using services or programs offered by cybersecurity companies (“No More Ransom!” initiative).

The most commonly known cyberthreat is loss or theft of personal data. We store a lot of data about ourselves in different networks because it is indispensable for a lot of our daily activities (online shopping, online platform for a bank account) or to utilize important services (healthcare information shared across hospitals and doctors, taxation and application for documents in government offices, certificates, permissions like passport, visa, change of residence, application for scholarships, government aid, pensions and so many more). One can
protect their information by using a VPN or Virtual Private Network when accessing their online accounts and information through a public network. VPN encrypts the flow of data creating the digital alternative of cable connection. Theft of information can cause even more harm when it occurs in case of large businesses or government agencies exposing private information of hundreds of thousands of clients. Another important step one can make to prevent data loss or theft is developing awareness of proper online behavior and the risks that use of cyberspace entails. This includes not opening emails from unknown sources or avoiding certain websites, installing an anti-malware software and regularly update its database, backup sensitive data, set complicated and illogical passwords and frequently change them. Companies can avoid these attacks by proper cyber protection set up by experts on their systems and by diligently training their personnel on the professional and moral dimensions of their actions in cyberspace.

Another threat which showcases how the online world can affect “real life” is cyberbullying. It has become quite a hot topic recently with several victims going as far as committing suicide because of the constant harassment of insensitive peers. Cyberbullying might be less physical but can be equally harmful because of the way social media infiltrated our daily life and relationships. Our online image/persona and our popularity in different social media platforms influences our face to face interactions and sometimes allows individuals to live life completely in the cyberspace (have relationships, communicate, employment). As a consequence of the addictive nature of digital entertainment, gaming, and social media breaking out of the influence of online bullying is very difficult as the online community usually exists parallelly to a real-life community. Cyberbullying can be countered the same way any bullying would be except it is more difficult because of how easy it is to share abusive information about somebody and the scale of the network that social media allows to maintain (no limit exists while in real life a network of 100 people of colleagues, friends and family can be considered average).

Another danger that can actually be prevented pretty easily is phishing. It is an attempt by cybercriminals to get the user to give out their own personal information like social security number, bank account password and so on by creating a web platform that looks deceivingly identical to a legitimate website. There is usually only a minor difference in the URL address and in the appearance of the website which the user doesn’t notice. When the user enters their login information the hackers usually quickly enter the real account with the acquired password and change it so after that the user won’t be able to access their own account even from the real website. By the time they regain access of their own account the information has already been
used: the bank account has already been drained or information has been stolen. A good way to protect yourself from this scam is to check every character of the URL address when entering websites with sensitive information.

Another relatively new area where cyberattacks can happen is the IoT or the Internet of Things. IoT is a collective name denoting all devices that can connect to a network in a household. It involves everything from the most obvious examples like a smart TV that allows the user to browse the internet on their device to some less noticeable examples like a fridge or a washing machine. This is not the most dominant threat as of now but definitely an emerging one which will become more and more prominent as we fill up our homes with smart devices that are capable of being remotely controlled and working together as a system via connecting to a (hackable) network. Some of these devices with less sophisticated functions and codes might seem harmless but if they get infected the malware will spread to other devices that are connected to the same network. In an imaginary scenario it is possible to infect a microwave with a very simple bot which will spread though the Wi-Fi network to one’s smartphone making the phone unusable by overwhelming it with executable orders. The owner of the smartphone will be surprised why his/her seemingly new smartphone became so slow all of a sudden. The bot will also infect other networks when the person brings his/her smartphone to the workplace and connects the device to the network there. Imagine the workplace is a bank, the system gets overwhelmed and freezes. In case of big companies even a few hours of skipped work means a loss of millions of dollars depending on the size of the company. Apart from causing harm in the form of loss of functionality or theft of data hacked IoT can lead to serious injury or death. The more these “smart” devices take over our lives the more we let control of our life be regulated by information technology. Soon many household chores will be completed with the help of or entirely by this web of smart devices. A smart thermostat helps save up money by reducing utility costs, a smart fridge orders food it senses we are running out of, a smart oven will start baking our dinner automatically so by the time we get home its ready, a smart car will microcorrect the steering wheel if the driver cannot keep the car in the lane or park the car without any input from the driver, a smartwatch calls the hospital for the user if it senses abnormal heart rate and so on. However, a pedophile can observe our child by hacking into the baby monitors, a terrorist attack can be orchestrated by taking over control of smart cars or the autopilot system of planes, a hacked printer can overheat and explode setting the whole office on fire, and it’s enough to disable an implanted pacemaker to let a person die from the daily heart rate fluctuations. Despite the dangers it is an evident upward trend to replace our “old”
manual household items with smart ones so countering, preventing this threat is of primary importance (index.hu Nemcsak adatokat...).

If our devices are infected by bots, they will become part of a large network of devices remotely controllable by cyber criminals similarly to ours (Kaspersky Lab: What is a Botnet?). Then this access can be resold to other criminals that will use our computers to infect or overwhelm other devices and websites or conduct illegal activity like purchasing illegal materials with our bank account, sending spam emails using our email account or store data on our device using it as a server. If our computer is being used like that it will become slower but most of the time other than that the attack will go unnoticed by the user. A computer that has become part of the botnet (robot network) can also be used to mine Bitcoin or other cryptocurrencies and thus generate income for criminals.

The botnet can also be used to carry out Distributed Denial of Service (DDoS) attacks. In this case the infected computers will send request to a particular website which will make it overload as it tries to respond to these. The basic idea is that more computers start to load the website that the capacity of the server that stores the website information. This will make the website load very slowly or become unavailable altogether deterring a regular user from further attempts to load the website. This is especially harmful for online businesses because it leads to loss of revenue (Kaspersky Lab: What is a DDoS Attack?).

3.2. Threats apropos of the public sphere, government-run systems and national security

In this paragraph I aim to examine the cybersecurity threats that affect state-run national systems and international relations between states. This section also concentrates on effects of state actions and policies on other states’ national policy or behavior.

Most of the threats listed in the previous section, concerning private individuals and firms, also apply to statewide systems and even can cause conflict and wars among countries. If the individual hacked is a prominent political figure and he/she has information of any nature that they don’t want to be disclosed about them, they become targets to blackmail and a vulnerability inside the state structure.

Furthermore, extensive systems like street lighting and traffic control infrastructure, a database of a hospital, or the taxation bureau database and network, if hacked, can threaten lives if they are incapacitated or their functioning is altered. There is no need to acquire nuclear material and technology to blow a destructive strike at any military superpower anymore. It is
sufficient to have computers and access to networks to hack a nuclear powerplant, cause malfunction which will lead to leak of nuclear material or/and nuclear explosion. As the materials used in the powerplant are highly radioactive and harmful for the human body a lot of functions used to stop the nuclear chain reaction (which would lead to explosion of the fuel rods) is operated by automated systems (e.g. cooling system). Stopping those is enough to cause a devastating disaster. One could argue that this is one of the reasons for getting rid of all nuclear technology, even the ones designed for non-military use and instead completely rely on self-replenishing energy resources like sunlight, wind, water and geothermal energy.

This can also be used as warfare against other countries by state and non-state actors alike. A real-life example of this is the Stuxnet virus. It was developed by the United States to attack Iranian nuclear facilities (index.hu Nemcsak adatokat...). Cyber warfare can be considered as a form of asymmetrical warfare which refers to the asymmetry in the tactics and tools used. Asymmetrical warfare increasingly characterizes conflicts in the 21st century. This strategy allows for a sharp jump in the number of potential actors that can endanger public security as well as traditional actors (defined as states by International Relations theory) who also utilize it in a growing tendency.

In the EU for example, along with the GDPR which I will introduce in the next section, a unified regulation was introduced to protect the security of network and information systems which are deemed to be essential to the societal activities and economy of Member States (it is upon the Member States to decide which are these). The NIS (EU Directive on security of network and information systems) defines two major categories that are affected by this regulation. The first one is the essential infrastructure providers like electricity or drinking water providers. The second category is online marketplaces, search engines and cloud storage. Companies and institutions involved in the above-mentioned activities will have to raise their level of security protection and are also obliged to report any cyber incidents that could obstruct them in providing these essential services to citizens. Furthermore, the NIS states that Member States have to set up national computer security incident response teams (‘CSIRTs’) or computer emergency response teams (‘CERTs’) – one central or even one for each sector of the economy - which will receive reports about incidents. Moreover, Member States also have to ensure that all CSIRTs/CERTs cooperate with each other in a European network (EU Network and Information Security directive). In Hungary for example this role is fulfilled by several such organs, the security of governmental sector is provided by the “Kormányzati Eseménykezelő Központ” (GovCERT) which is part of the national cybersecurity organization network headed by the “Nemzeti Kibervédelmi Intézet” (NKI) or the National Cybersecurity
Institute which is supervised by the “Nemzeti Elektronikus Információbiztonsági Hatóság” (NEIH) (Official Journal of the European Union: DIRECTIVE (EU) 2016/1148).

3.3. Security versus privacy

This is an eternal question that concerns all areas of state provided security. The main question is whether privacy can be considered a human right and if it is then is it more important than our security. In the Universal Declaration of Human Rights it is explicitly stated that a Right to Privacy exists\(^2\) but it is also commonly known that human rights can be derogated in case of emergency. Do we have a right to choose privacy over personal security? Not necessarily. If our personal security is breached it can mean a threat to the whole community. On the other hand, it is important to keep in mind that even if we give up our privacy the state or cybersecurity companies won’t necessarily be able to provide us with security at least not in a proportional manner. In fact, the opposite can happen. When a lot of data about citizens or clients is collected together it will become a highly desired target for criminals. Although the data will be equipped with increased security there is no flawless system so sooner or later it will be breached. Leak of highly sensitive information can be the origin of further disastrous implications.

For this reason, the General Data Protection Regulation (GDPR), the new EU legislation regarding collection and treatment or user data and privacy is an important step, but it comes at a cost of limiting opportunities for providers, websites, businesses. It also affects the users as the collected data was usually used to personalize the content presented to them – providing a more relevant and practical experience to the user and increasing the success rate for companies as they reached a filtered target audience. The GDPR is effective since May 25\(^{th}\), 2018 and is essentially not a revolutionary change in terms of novel rules unlike the buzz around it would suggest. It is outstanding because it raises the threshold for data protection and also increases the penalty for overstepping it. Although it is quite costly for companies to readjust their policies regarding data treatment (which is especially harsh on small- and medium enterprises) on the long run it is expected by lawmakers to converge data protection laws in European Union Member States making the EU cyberspace a truly unified market.

\(^2\) Universal Declaration of Human Rights (1948) Article 12: “*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*”
The GDPR gives more control to the user over what personal data is collected about them and obliges the companies to make their activity regarding user data transparent and easily accessible to clients. It furthermore restricts data collectors on the exact type of data they are allowed to gather. It has to be indispensable to provide the services the user has turned to the company for. Furthermore, firms and institutions are obliged to delete the data after the ground for data use has been terminated and notify the authorities and the users in case their data was hacked or leaked within 72 hours of the incident (General Data Protection Regulation (GDPR)).

The problem with GDPR is that while it identified the above-mentioned regulations which are in theory very useful for a better protection of personal information used in the cyberspace, in practice it is unclear exactly how to operationalize these rules. The GDPR does not describe the exact tools or formats to be used which makes the whole procedure complicated and difficult to carry out/costly when hiring data protection specialists. It is not uncommon to see advertisements for companies named “Compliance Kits” which “include a template Privacy Risk Assessment Procedure & Questionnaire you can download and easily customise for your organisation for use when conducting Privacy Impact Assessments or privacy audits, as well as a template Privacy Policy” (Johnston, 2015). From this perspective the GDPR is unnecessary bureaucracy which places a major burden on businesses. These extra procedures will occupy companies and institutions hindering them from effectively carrying out their duties and functions. Furthermore, these extra costs are likely to be transferred on the clients. It is also important to note that if these regulations could be reasonably followed one or two decades earlier then today IT has developed so dynamically that the personal data in question are used for so many purposes and stored on so many platforms that deleting them entirely (on the request of the user or because of the termination of legal basis for their use) is virtually impossible to ensure. Today one single piece of data, say a name or an ID number, is stored in the database, backed up in another, was sold to advertising companies after alleged anonymization, mentioned in emails like confirmation of registration (which is therefore stored on the server of the email provider and out of reach of the original company). Consequently, the saying that once something is posted on the Internet it cannot be really deleted holds true. It also doesn’t help that online storage is ridiculously cheap and even data we think nobody would find useful is stored as it can become useful as part of big data to explore trends and tendencies. Things an individual can do is basically not enter data into any IT device. However, with the way our lifestyle is developing, beyond convenience and efficiency, it becomes increasingly impossible to entirely avoid creating an online profile for ourselves, even if only to fulfill our civic duties (like having an ID). Even if we enter pieces of data that in theory
doesn’t make us identifiable, in hands of IT experts these entries can be connected giving a full picture of an individual. For example, taxation and health records connected with geolocation data and social media posts can give a complete picture about a person. It could make the situation a bit better if we separate our private and professional profiles and store as many data as possible on a local storage disconnected from any network instead of using cheap, widely available and conveniently accessible cloud storage.

The raise of security protection and obligatory reporting of cyber incidents prescribed by both the NIS and the GDPR might seem to overlap at first, but their focus is different. While the latter concentrates on treatment of users’ personal data the former on the operation of companies themselves. Moreover, the GDPR is a regulation thus it has to be directly applied on the national level while the NIS is a directive therefore it has to be first adopted into national legislation (EU: Regulations, Directives…). However, both aim at bringing cybersecurity standards in the EU Member States to a uniform level, raise and make cybersecurity policy up to date, help companies, institutions and users adjust to the 21st century cyberspace situation, and facilitate cooperation of national crime persecution organs Union-wide as part of the justice and home affairs policy of the EU. A concern raised by IT experts however is that the IoT is not covered by any of these regulations so that area remains unregulated and thus unprotected despite carrying significant risks as it has been previously explained in this paper (index.hu Európa felkészül…).

Following the review of cyber threats, I will now move on to the conceptualization of my research question and explain why countering the previously mentioned threats as well as other security challenges in Europe is approached from the perspective of NATO and its collective defense clause, Article 5 of the Washington treaty. In other worlds, I will outline my reason for choosing NATO as my unit of analysis instead of the similarly prominent EU by detailing European security architecture.
4. NATO as a centerpiece of European security and Article 5

Let’s take a step back and really elaborate on why we are taking about NATO when it comes to the security of Europe (albeit its delimitation is questionable). We have to put the emergence of a collective security alliance in Europe in the context of the post WWII environment and the rise of the communist bloc. Europe was in ruins so the formation of an effective security, especially military security organization without the participation of the US would have been unimaginable. The North Atlantic Treaty Organization was established in 1949 by Belgium, Canada, Denmark (the Faroe Islands and Greenland), France, Iceland, Italy, Luxembourg, Netherlands, Norway, Portugal, United Kingdom, and the United States. Later, its membership has expanded and came to include many former Warsaw Pact members. As of today, the NATO boasts 29 members with Greece and Turkey joining in 1952, Germany in 1955, Spain in 1982, the Czech Republic, Hungary and Poland in 1999, Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, Slovenia in 2004, Albania and Croatia in 2009, and finally Montenegro in 2017. The most important clauses in its founding document, the Washington Treaty are arguably Article 4 and Article 5.

Article 4 goes as follows: “The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.” While this clause does not in itself imply any collective defense action only consultation, nevertheless we should highlight the cases which constitute a matter of interest when it comes to preservation of security. It is very much relevant from the perspective of cybersecurity as cyberattacks can truly compromise the security and political independence and indirectly the territorial integrity of states as it has been outlined in the previous chapter.

Additionally, Article 5 states that „The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.” Article 5 explicitly limits the cases in which this collective defense clause is activated to armed attacks. However, in an
age when nuclear launch codes can be hacked shouldn’t cyberattacks be considered armed attacks as well? I would argue that while certainly such an act signals a hostile intention in itself it cannot be considered an armed attack. On the other hand, we could examine if a cyberattack is capable of a disruption and destruction on the scale of conventional and nuclear arms attacks and then it would have to be included. If we formulate the dilemma like this, we are using the narrow definition of security and it cannot be denied that the world has changed so much it is just not sufficient anymore. To keep up with the changing, complex and interwoven nature of today’s world affairs, politics, economy and society the understanding of security has to be expanded. Therefore, instead of trying to explain how cyberattacks can be considered an armed attack, the definition itself and the treaty has to be modified. If the NATO wants to stay effective and relevant of course. And that isn’t so obvious as some very influential leaders show an apparent lack of enthusiasm when it comes to the organization, furthermore consider it – albeit unofficially – a burden. This leader would foremost be Donald Trump, US president who considers his country to be a net contributor of security benefits in terms of the operation of the organization (does not equal budget). The treaty itself has actually outlined the process of reviewing of the founding document in Article 12, setting the soonest possible date for that 10 years after it has entered into force. Although Article 12 does not oblige the Member States to engage in such a review, nevertheless it implies that the makers of the treaty have envisioned the likelihood for a need to modify the rules and principles of the organization in about a decade after its creation. We hear so much about the need for UN reforms and the reforms regarding the budgetary burden sharing in the NATO but the basics constituting the core of NATO are also in need of an update.

Moreover, it has to be mentioned that this collective defense clause is relatively weak legislatively speaking. Especially the “such action as it deems necessary” part makes the obligation so broad that in the end it might mean nothing at all when it comes to specific actions. In fact, the only case when Article 5 has been invoked before was the 9/11 terrorist attacks. Then again, this vagueness provides the treaty with much needed flexibility and probably allowed the treaty to remain relatively unchanged for so long. Indeed, there have been a total of three official footnotes in the 70 years of its existence, all insignificant to the substance matter of the collective defense clause.

Moving on to its membership it is evident that the NATO is very much a European security organization: firstly, there is a high degree of overlap between its membership and that of the EU and secondly, Article 6 defines that the treaty is only applicable with regards to the territory of the Member States In Europe and North America (although the later aspect has
changed recently as the NATO decided to undertake out of area missions but exclusively if it has been preceded by an armed attack against the territory of the Member State).

It must be remembered that the NATO is only one pillar of the European security architecture, even if the most significant one. I have to speak a few words about the WEU and the defense cooperation within the framework of the EU.

Actually, the NATO was not the only attempt of the European countries in terms of security cooperation however “their own” common defense organization has failed even before it could be launched. Following the successful integration on the economic field with the establishment of the Coal and Steel Community in 1951 the (western) European countries were eager to expand the cooperation to the political and military field. The European Defense Community (1952-54) and the European Political Community (1953-54) were short lived projects that failed to pass the ratification stage. The ambitious plan for supranational integration had to be scaled down. Nevertheless, military cooperation manifested in a less “intrusive” (into national sovereignty) organization: the Western European Union was established in 1955. It had a legal personality of its own. It has existed until 2005 when it was merged into the EU.

The EU had its own branch of security related cooperation. Defense cooperation was already included into the founding document of the EU. The Maastricht treaty (1992/1993) determined the EU structure to consist of three pillars, the second of which was the Common Foreign and Security Policy. The expansion and specialization of this CFSP in the consequent Amsterdam treaty ultimately led to the emergence of the European Security and Defense Policy within the CFSP pillar and its merger with the WEU. In 2009, the Treaty of Lisbon renamed the ESDP to Common Security and Defense Policy. The CSDP is also a collective self-defense organization and it contains a mechanism called the Permanent Structured Cooperation (PESCO). PESCO is a framework aimed at structural integration of the national armed forces of 25 Member States. The CSDP can be considered a precursor of a full-on European Defense Union. The two treaties signed in Lisbon both contain a collective defense clause: the Treaty on the Functioning of the European Union Article 222 “Solidarity clause” and the Treaty on the European Union Article 42.7 “Mutual Defence Clause”. The latter remains short and very broad on specifics of cases when the collective defense mechanism is triggered simply referring to armed aggression and aid by members in accordance with the UN Charter. The former however is a very detailed and thus strongly binding piece of legislation with the specific goal to fight terrorist attacks and natural or man-made disasters.
The cooperation between the national forces of the European nation states, the EU ESDP and the NATO remains vital today as it has become greatly interconnected over the years. Firstly, the Maastricht treaty assigned the WEU “...to elaborate and implement decisions and actions of the Union which have defence implications”. Consequently, the NATO has developed the European Security and Defence Identity (ESDI) back in 1996 with the aim to allow WEU to use NATO resources (forces, intelligence, equipment) to carry out its operations. In the Amsterdam Treaty (1997/1999) the functions of the WEU were integrated into the EU which practically meant the end of WEU even though formally it ceased to exist only in 2005. To meet the tasks transferred to the EU by the integration of WEU, the Member States decided to set the so called ‘Helsinki Headline Goal’. According to this document the Member States voluntarily undertake the development of rapidly deployable and sustainable forces that combined together can serve military objectives outlined in the “Petersberg Declaration” of WEU. The Petersberg Declaration sets out a range of “post-Cold War tasks” like humanitarian operations and peace-keeping. Further buildup of the European security and defense architecture occurred during the consequential EU council meetings. Nowadays the EU has an extensive operational structure (plus a US-led Combined Joint Task Force currently engaged in the fight against ISIL), various military forces (EUROCORPS, EUFOR, EU Battlegroups, European standing naval force, European Gendarmerie Force, furthermore Forces Answerable to the WEU were obviously transferred to EU), a long list of private defense companies (mainly British and French), a European Security Strategy and various operations undertaken worldwide.

In terms of EU-NATO integration a security agreement has been signed in 2002 in Prague called the “Berlin plus agreement” which made NATO assets and capabilities available for EU-led operations. Furthermore, in 2010 at the NATO meeting in Lisbon an agreement has been reached regarding a new approach. Smart Defence is a way of generating defense capabilities necessary to carry out military objectives. Due to the cooperation acquisition and maintenance of capabilities will both be cheaper. Among the most important capabilities cyber defense was mentioned, showcasing the importance of this sector on the EU’s and NATO’s agenda. Cooperation has been tightened and both consequent meetings: in 2012 in Chicago and in 2014 in Wales. Although the EU is certainly creating an increasingly developed and independent security architecture but it is still lacking in the capabilities department compared to NATO. One day the two structures might become of equal importance in countries that have an overlap between membership with the two organizations. However as of today we can observe that in practical terms the EU is relying on NATO just as much as before.
Now we see why the NATO is the most relevant organization when it comes to security of Europe even if that might change in the future, especially if EU manages to tighten and deepen cooperation among the Member States. It is actually more likely to happen now if the UK leaves, as it has always been a country that opted out of and strived to limit any initiative connected to deepening the integration regardless of the sector in question.

In the next chapter I am going to introduce the cybersecurity architecture of NATO as well as the current stance of the international community on the application of Art. 5 in cases of cyber-attacks.
5. Cybersecurity in NATO

In this section I will introduce the cybersecurity policy of NATO as cybersecurity receives more and more attention from the organization.

The primary question we must discuss before diving into NATO cybersecurity policy is whether Europe is threatened. If yes, how? Are cyberthreats significant enough to threaten the security of Europe? There are so many layers to security that it is really difficult to delimitate specific areas that need special attention. Security can mean - according to the strictest, most narrow definition – military security. If we use this definition, then the most realistic threat currently is an attack from Russia. Russia has showed multiple times that it is willing and capable of using cyber aggression as part of its hybrid warfare tactics. In terms of an armed attack the countries that are in real danger are the ones geographically positioned near Russia, economically dependent on Russia or the EU, lack substantial military power or have a past under Russian rule or influence. There are several countries that fit these requirements. These are the small Baltic counties Estonia, Latvia and Lithuania. These countries themselves can also feel that there are dark clouds gathering above their security and sovereignty. This attitude is evident if we look at the announcements and public speeches of top government officials of these countries and NATO military experts or if we remember the 2007 series of cyber-attacks by Russian hackers on Estonia. Other countries that also belong to this hypothetical group of threatened countries are the Scandinavian countries Finland and Sweden. To somewhat counter and prepare for a Russian attack these countries -although did not join – made steps to move closer to NATO. Although surely, they are familiar with the security dilemma (outlined below), the aggressive behavior of Russia must have pushed them towards this decision.

The security dilemma, a concept in the science of International Relations declares that extension of an entity’s military capabilities aimed at increasing its security unwillingly threatens other countries which in turn will also engage in military buildup. The base assumption is that every party sees their own actions as defensive and the others’ actions as offensive. This leads to a dangerous spiral of increasing tension which is like a ticking time bomb. In such an atmosphere even the smallest, otherwise harmless event can lead to a major confrontation. Military is an industry and war is a market. Sadly, the military industrial complex is a trillion-dollar industry which obviously does everything to create demand for its products. Once a country builds up a substantially sized military it will inevitably be tempted to use it. Creating and maintaining an army and equipment is very expensive so the country will look for a “use” to justify the spending. In both democratic and authoritarian countries, the top political
layers are strongly interwoven with the elites of the military industrial complex (or they are outright the same like in China).

This security dilemma can be observed in the relationship of Russia and NATO. Back in the days of the Cold War the Soviet Union (who’s legal and politico-economic successor is the Russian Federation) and the United States engaged in an arms race which resulted in such a huge military buildup of both conventional and nuclear weapons that it endangered the safety of the whole planet. The Warsaw Pact and its western counterpart, the NATO were military alliances aimed at unifying the forces of their respective blocks to better protect themselves from the other. The Cold War has however ended with the dissolution of the Soviet Union, the Soviet block and the termination of the Warsaw Pact. Russia became a democracy, a capitalist country – although this process seems to be slowly undone by the single party rule (not legally but practically) and the economic rift that appeared between Russian and the “rest” due to the sanctions enacted following the annexation of Crimea and the East Ukrainian strife. Following that NATO struggled to find a new purpose. To redefine itself it explicitly stated that it is not a coalition against Russia and took up broader tasks and conducted its missions in a wider area than the exact territory of its the Member States. It is therefore imperative to recognize the effects of normalizing cyber-attacks as part of interstate conflicts or war. Technical buildup and the creation of a solid legal background for the use of force in self-defense on the side of NATO can be seen as a sign of intent, as preparation for aggression from the perspective of actors that are not in NATO or its allies.

Russia has already showed signs of aggression in Georgia and Chechnya but those events seemed far enough from the EU not to concern the West that much and close enough to Russia to be considered its sphere of influence. With the Ukraine crisis and the annexation of Crimea however Europe got a wakeup call. This move led to a significant shift in attitude of the West towards Russia and was called by some the start of a new Cold War. Russia is not a superpower anymore; it cannot exert as much influence and deploy military power directly as the Soviet Union once did. But it is still one of the strongest military powers in the world, let alone in Europe. Therefore, smaller countries like the aforementioned Baltic and Scandinavian states don’t stand a chance against it unless they are part of an alliance. As discussed previously in this paper, the nature of warfare is changing and so are the actors. Russia relies a lot on cyber warfare because it is cost effective, and because of its novel nature a cyberattack cannot clearly be identified as aggression like a conventional attack. The problem of attribution is very convenient for Moscow that always disassociates itself from the actions of Russian hackers, nevertheless the Russian government never allowed inspection on its soil to trace back the
aggressors in the cases of the 2007 Estonia, 2008 Georgia or 2014 Ukraine cyber-attacks cases. Legislation isn’t comprehensive enough in this field and Russia and other authoritarian countries like China use the cyberspace to terrorize their targets. It is also much harder to prove who is behind an attack which is also very convenient to the perpetrator. The victims will likely not accuse the actual source of the attack as the Russian leadership – if they are behind the attacks as it is suspected – act through hacker groups by financing and giving orders to them. Beyond the actual damage these attacks act on the psychological level. These attacks make sure to remind the victims that they are on Russia’s list of targets. Living in constant terror leads to military buildup and to military grouping (like the tightening cooperation with NATO). This takes away resources from other sectors which could uplift the country e.g. spending on improvement of education, healthcare, infrastructure, aid to small and middle enterprises, startups and so on. Russia is creating insecurity in Europe from use of “long range precision fires, to surrogate fighters, to cyber-attacks, and misinformation intended to shape and influence domestic and international opinion” (Matallana, 2017, pp. 10-11).

Apart from the Baltic and the Scandinavian states which feel directly threatened by Russia, there are other countries that also seem to be targets of - maybe not aggression but - influence by Russia. Countries can be grouped together based on the type of rhetoric Russia tries to use to gain influence. The first one is the Pan-Slavic group. Slovakia and the Check Republic belong here. Here Russia tries to play the sympathy card by reminding these countries, politicians and voters alike, that they have a common history, culture, similar language and values. Based on the analysis of discourse appearing in the media of these countries this group of countries resisted well Russian strategy of “information-warfare”. Another country that is seemingly targeted by Russia is Hungary. Here Moscow tried to use the revisionist desires that some parts of the society and of the political elite still retain. It might not signify a return of territories lost by Hungary after WWI but rather a bigger autonomy for those “outer territories” within their “new” state and greater participation of expatriates in the social, political and economic life of Hungary. Hungary has lost more than 70% of its territory in the Treaty of Trianon, the peace treaty signed to conclude the WWI. In terms of objectivity and resistance to foreign influence in the form of Russian propaganda the Hungarian media receives a mixed grade. On one hand the government close media did have a biased, Russia-friendly take on the Ukrainian crisis and other Russia-related news. On the other hand, large online newspapers and media stayed more or less neutral showing all the different perspectives to these events (index.hu Javában zajlik...).
With all that said I have to turn back to the definition of security that I have discussed in the beginning of this section. If we consider the broader definition of security, it will paint a very different picture for the EU. It will reveal that there are countless threats that the EU has to face from migration which threatens social security to the rise of alternative economic centers like China that might mean turbulent times for the economy of the single European market. And that is just half of the troubles. The Brexit is really just the tip of the iceberg – it is a symptom showing that there are still internal problems, disparity and disagreement among the Member States of the EU, cleavages between the different cultures and customs. If we concentrate on this, broader definition cybersecurity becomes extremely relevant to European security, more so in the light of the European security architecture and its most recent challenges. I have to make it explicitly clear that there is no negative bias against Russia in the choice to analyze (in a further chapter) the Russian meddling with the 2016 US presidential election to discuss the reinterpretation of NATO commitments undertaken in its founding document. It just so happened that the most advanced security mechanism providing Europe with security, NATO had to face one of its biggest challenges in recent years due to a game changing cybersecurity attack on its most powerful Member State, the USA.

The NATO leadership can certainly sense that it is time to apply a broader understanding of security in the 21st century. If we look at its organizational buildup, we can see that countering cybersecurity threats is already on the list of top priorities. To demonstrate this, I will now briefly introduce NATO’s cybersecurity architecture and its history.

NATO is the most developed collective security organization in Europe. It could be argued that its survival after the end of the Cold War is partly the reason why the EU has yet to develop an advanced military cooperation (although the situation seems to be slowly changing). NATO has always been concerned with maintaining security and stability in the Transatlantic region via deterrence of collective self-defense, crisis management and cooperative security. As it was outlined previously, collective self-defense is activated if any of the Members suffers from an armed attack. Deterrence is still greatly relevant today in the era of the rebirth of the West v. Russia antagonism, and the evident eagerness to use cyber-attacks by both sides. Yes, NATO is considering the buildup of offensive cyber capabilities to use as deterrence. Today NATO Member States, especially the Eastern European ones fear another large-scale conventional war. Crisis management was mainly developed in the 1990s after NATO has redefined itself and its core tasks. It has emerged to counter problems caused by non-state actors and failing states such as terrorism, peace-keeping efforts and migration and Internally Displaced Persons. The cooperative security pillar deals with leveraging benefits from
cooperation with other organizations, the EU, other national actors, the industry and NGOs. (Matallana, 2017, p. 8).

The first steps towards a comprehensive cybersecurity policy were taken at the Prague Summit in 2002. It has followed attacks suffered by NATO during its 1999 air campaign in Kosovo and the cyberspace related dimensions of the Afghanistan mission. In the 1999 Balkan wars a Russian hacker group, called From Russia With Love, spearheaded the attacks after the Russian and the Chinese embassies in Belgrade were bombed by NATO – accidentally (Szentgáli, 2013, p. 83). At the summit the Cyber Defense Program was adopted. As a result of the program the first cybersecurity specific body, the NATO Computer Incident Response Capability (NCIRC) has been established. It is tasked with protection of NATO’s own networks in case of a cyber-attack (Healey and van Bochoven, 2012, pp. 1-2). The Technical Centre of NCIRC is responsible for detection of intrusions into NATO’s own networks.

After the attacks against Estonia in 2007 and the Russian-Georgian conflict a year later NATO has decided to place more emphasis on cybersecurity. As a consequence, in January 2008 the Alliance developed its first Cyber Defence Policy (Szentgáli, 2013, p. 84). At the 2008 Bucharest Summit the Alliance has greatly expanded its cybersecurity structure and capabilities. The first institution to be created is the Cyber Defense Management Authority (CDMA). It is responsible for initiation and coordination cyber defense in case of a cyber emergency, review capabilities of NATO and Member States and conduct security risk assessment. Basically, the CDMA would be the government if NATO cybersecurity architecture would have been a nation state. The CDMA is placed under the supervision of the Cyber Defense Management Board (Healey and van Bochoven, 2012, p. 2).

Secondly, the organization has set up the Cooperative Cyber Defense Center of Excellence (CCDCOE) dealing with issues of education, research, legal guidance, information pooling and cooperation in Tallinn, Estonia (Matallana, 2017, p. 12). Already, the location of this center carries a message in itself which is not difficult to read considering the previously mentioned categorization of European countries under Russian threat or influence. It should be noted that this symbolic message seems to contradict NATO’s previous denial of Russia still being the enemy against which the treaty organization stands. There are 15 further centers of excellence operating all coordinated by the Allied Command Transformation (ACT) (Szentgáli, 2013, p. 84). The NATO Allied Command Transformation (ACT) is responsible for standardization and interoperability of networks among Member States (Matallana, 2017, p. 19).
Thirdly, as a result of the Bucharest Summit, NATO has initiated the development of Rapid Reaction Teams (RRTs) at the request of Member States. Operational by 2012 the RRTs can be rapidly deployed to assist particular Members that request assistance in case of a cyber-attack (Healey and van Bochoven, 2012, p. 2). RRTs operate subordinated the NATO Computer Incident response Capability Technical Centre (Szentgáli, 2013, p. 85). Apart from the NATO level organization, Computer Emergency response Teams (CErT) were established on the national level (Szentgáli, 2013, p. 84).

In 2010, NATO adopted a new strategic concept at the Lisbon Summit however many of the base assumptions outlined in the strategic concept are now “incomplete or have significantly changed” (Matallana, 2017, p. 8). At the time both NATO’s Strategic Concept and the 2010 Lisbon Summit Declaration focused on the defensive capabilities (Healey and van Bochoven, 2012, p. 2). NATO exercises the “deterrence by denial not punishment” idea by which it deters any potential aggressor as its cyber defense is impenetrable or it can recover from damages so quickly attacking would be pointless (Healey and van Bochoven, 2012, p. 5). On the other hand, deterrence by punishment would require development of offensive capabilities even if in the cyber domain the border between defensive and offensive is the most blurred. Currently NATO itself does not but several of its Member States do have offensive cyber capabilities which could be used to create the core of NATO’s own offensive forces. “NATO offensive capability already exists, but it lies within the national militaries, not in any collective NATO agency or unit” (Healey and van Bochoven, 2012, p. 7).

With the new Strategic Concept the Global Commons project was launched supervised by the Allied Command Transformation. It is aimed to address “geographical and virtual dimensions which cannot be associated with any specific country: however, they play a crucial role in NATO’s security” (Szentgáli, 2013, p. 85). These can be airspace, outer space, oceans and seas, and cyberspace.

To bring the Cyber Defense Policy in line with the new Strategic Concept defense ministers at their meeting in 2011 in Brussels decided to accept amendments. An Action Plan was published in June 2012 has outlined the main areas of focus for the coming years for NATO’s cyber policy with the goal to bring the Strategic concept into practice (Szentgáli, 2013, p. 87). However, it has continued to concentrate on prevention, resilience, and defense, just as it does so at the present time. The main ideas voiced the 2012 document are (1) protection of NATO’s own networks, (2) increasing and centralizing NATO’s own cyber defense capabilities, (3) setting minimum cyber defense capability targets for Member States, (4)
assistance to allies to meet these requirements, (5) as well as cooperation with other international organizations, the private sector, and academia.

CDMA has been succeeded by the Cyber Defense Management Board (CDMB) which continues to encourage the realization of these headline goals by signing so called memoranda of understanding with the respective authorities of each Member State.

The Defence Policy and Planning Committee in Reinforced format or DPPC(R) chaired by the Deputy Secretary General is responsible for long-term planning of cyber capabilities (Healey and van Bochoven, 2012, p. 3).

This organizational structure with its elaborate policy areas mandated to different boards and committees, and specifics laid out in a comprehensive manner in one document streamlined the cyber security policy management. It also gave much needed clarity to the process of invocation of collective defense (Art. 4 and 5) while allowing the organization to maintain ambiguity about the thresholds. NCIRC, a body made up of technical experts starts to escalate cases to first the Cyber Defense Management Board and then the DPPC(R) which finally reaches the highest, purely political level decision making body the North Atlantic Council (NAC). The NAC makes the final decisions in case of any emergency not only the cyber related ones. Therefore, cyber conflicts aren’t a technical matter that NATO automatically assists the Member States with but a political matter as well. If it is sufficiently grave, the NAC can choose to invoke Article 5 (although it is unlikely).

Healey and van Bochoven have compiled the factors (the first three based on Thomas Wingfield’s work) the NAC would probably look at in the unlikely case it would decide to invoke Article 5: (1) scope as for geographical coverage of the attack, (2) duration, (3) intensity, and (4) presence of an external actor as an attack from a domestic actor is akin to self-determination (Healey and van Bochoven, 2012, p. 6).

The formulation of NATO’s cyber policy is carried out by the Defence Planning Committee which is continuously submitting proposals to the North Atlantic Council, including cyber defense. Furthermore, there is the NATO Communication and Information Agency (NCIA) which operates NATO-wide and provides centralized protection to all bodies. It is a successor of the NATO Consultation, Command and Control Agency (NC3A). Those functions which require cyber expertise are performed by the NATO Computer Incident response Capability Technical Centre. In addition, in 2012 a Cyber Threat Awareness Cell was created to pool intelligence (Szentgáli, 2013, p. 87).

After the 25th summit in Chicago in 2012 cyber capabilities were indicated as vital in a document about NATO defense capabilities.
NATO had to face challenges again in 2014 as cyber-attacks accompanied the Russian invasion of Ukrainian Crimea. At the consequent 2014 Wales Summit the heads of state and government made three announcements with regards to NATO’s policy towards cyber-attacks. Firstly, they confirmed that cyber defense is part of collective defense in accordance with the Strategic Concept. Secondly, they declared international law would be applied in the cyber domain. Lastly, they announced that a cyber-attack that met the threshold of a conventional armed attack as an act of war could trigger a collective defense response under Article 5 of the Washington Treaty (Ghavaml, 2016, p. 21).

An enhanced cyber defense policy was published in 2014 in which NATO made it clear that Article 5 could be invoked for a major digital attack. However, that would happen after a political process of decision-making with unclear thresholds. It is a mystery whether that actually increases or decreases its deterring force. NATO does not have a standing cyber defense force per se, its structures now cover the political, operational, and technical challenges of cyber defense (Ilves et. al., 2016, p. 129).

In the Warsaw Summit Communiqué in 2016 the Alliance has declared cyberspace its fourth domain of military operations. This announcement has normative implications. Such statements “could endanger the free circulation of information in cyberspace should the use of cyber capabilities in interstate warfare become common practice in the future” as cyber component is being incorporated into traditional norms and rules of interstate conflict and international law (Spiegel, 2017, pp. 3-4).

Moreover, NATO also conducts regular conferences and meetups for the Member States where the topic of cybersecurity is becoming increasingly prominent.

In addition, NATO also holds trainings and simulations in several categories in which Member States can compete with each other. One of these held in 2016 part of the Locked Shield series, a real-life cyber war simulation and one of the biggest of its kind has been won by Slovakia for example. Past exercises include: Baltic Cyber Shield 2010, Cyber Coalition since 2008, Locked Shields since 2010 and Crossed Swords since 2016 (CCDCOE website). The exercises are run or aided by the CCDCOE in Tallinn.

The Smart Defense Initiative was created to ensure efficient use of the minimal budget in the face of wavering commitment to defense spending in the Member States. It has been at the forefront of encouraging Member States to increase cooperation, specifically to “develop, acquire, operate and maintain military capabilities to undertake the Alliance’s essential core tasks agreed in NATO’s Strategic Concept” (Matallana, 2017, p. 14). Out of the 143 projects of the initiative currently three involve cyber defense. The Multinational Cyber Defence
Capability Development Project (MNCD2) has been created to improve the members’ ability to detect malicious activity. A Cyber Information and Incident Coordination System has also been developed by Canada, Denmark, Norway, Romania, and the Netherlands to facilitate sharing of sensitive information. The Malware Information Sharing Platform allows Members to share technical information without having to expose the details of the cyber-attack itself\(^3\) (Pernik, 2014, p. 7).

In terms of cooperation between NATO and other international organizations, primarily the EU and with other partners inside and outside the Transatlantic sphere all documents detailing cyber policy recommend NATO to continue and enhance coordination and cooperation. Moreover, a closer link is encouraged between the private industry and users on one hand and the national governments and cyber policy related bodies on the other. Primarily because the industry has the most advanced technology and the biggest capacity to act in cyberspace and because users can be directly affected and even used in a cyberattack against or on the side of the national government. Secondly, because the cyber dimension is a truly borderless space therefore delimitating it would be a vain attempt.

The main difference between NATO and the EU in terms of their legal background on cyber policy is that NATO has a very broadly worded treaty which has not been modified while the EU has detailed provisions enshrined in legally binding treaties which are revised often. Both the EU and NATO consider cyber security a policy area of strategic importance. They both prioritize the defense of their own networks for now leaving the Members States with the responsibility/autonomy to manage their national IT security. On the technical side the two organization are apt at different sides of cyber security and therefore would best function as each other’s complementors. NATO focuses on security and defense while the EU concentrates on broader, non-military issues such as Internet freedom and governance, online rights and data protection and other internal security aspects (Pernik, 2014, p. 1).

On the more technical side a cooperation with the EU would probably mean a cooperation with the European Defense Agency (it launched a cyber defense program in 2011) and the European Network and Information Security Agency (ENISA) which monitors EU’s own networks and reports any issue to the Commission, organizes joint exercises, and engages in information dissemination at conferences, etc. (Szentgáli, 2013, p. 90). It is important to avoid duplication even more so as the two organizations’ memberships overlap. More efforts

---

\(^3\) The Transatlantic Defence Technological and Industrial Cooperation is a partnership to increase cooperation with the private industry (Pernik, 2014, p. 7).
have to be made in this direction as despite the regular NATO-EU working level meetings “tangible results have been modest” (Pernik, 2014, p. 9).

Moreover, the NATO Industry Cyber Partnership contributes to tightening the ties of NATO with the private industry (Spiegel, 2017, p. 45) which in all the Member States has the biggest pool of resources and knowledge.

It is important to speak a few words about the post-positivist implications of NATO’s activity in cyberspace, and its way of formulating cyber policy, as well as it approach to the cyber domain as just another dimension for military activities. Spiegel argues in her thesis that the Alliance is producing not only security practices but normative discourses as well that focus primarily on the technical and operational challenges of cyberspace, which in turn determine the legal challenges of attribution and the categorization of cyber-attacks as armed attacks (Spiegel, 2017, p. 11). NATO seems to pay no attention to the structural consequences and does not recognize its own influence in creating the very environment which in turn determines the challenges NATO will have to counter. Correspondingly, NATO’s and the other important actors’ attitude and actions in cyber warfare could change the role of civilians in armed conflicts in the future (Spiegel, 2017, p. 12). The CCDCOE often refers to the modern society as ‘Information Societies’ because people’s life is so immensely connected to the virtual. Likewise, many interactions between citizens and the government occur in cyberspace (Spiegel, 2017, p. 17). This argument shows the other side of the coin and reminds us that providing something negative such as cyber-attacks with legal recognition might contribute to its proliferation. It is also likely to lead to restriction of our online liberty as securitization always leads to attempts by the authority to gain increased supervision over the securitized domain.

Spiegel perfectly grasps the essence of the problem saying “the organisation focuses on legal and technical solutions to the security of cyberspace, neglecting the political implications of militarising cyberspace in the name of security” (Spiegel, 2017, p. 21). Therefore, the question has two aspects: the legal side (Is cyber-attack an armed attack?) and the normative (Should it be?).
6. International legal background: invocation of Article 5 by a cyber-attack

NATO has made the decision at the 2014 Wales Summit to allow the North Atlantic Council (NATO’s main political decision-making body) to take a decision on a case by case basis. Political decision making can be extremely tedious and slow at times, while a presence of a clear and binding legal rulebook would make this process automatic and put it in the hand of experts. Most politicians know little about codes and protocols which makes them dependent on cyber experts’ opinion anyways. If NATO is already using up resources, it might as well make the best of it. As it was highlighted my Matallana “the relevancy of NATO will in large part be shaped by its ability to act decisively within the cyber domain” (Matallana, 2017, p. 19).

In addition, the tendency of improving technical capabilities and giving bigger ad hoc political decision-making power without proper legal background is problematic.

If we analyze the text of Article 5 of the Washington treaty it becomes evident that the creators left the wording of the collective self-defense clause vague on purpose. Although it is not possible to confirm with legal certainty that cyberattacks can be considered an armed attack (as this decision is currently left to be made on a political basis) and consequently entitle the victim Member State(s) to invoke Article 5 nevertheless we can rely on other legal documents to aid political decision makers in their search for clarity. One way is to rely on the commonsensical solution to decide based on the scale of the destruction or damage inflicted by the cyber-attack. However, what happens when the attacked Member State’s cyber preparedness is high, and it could successfully counter or mitigate the negative consequences of a cyber-attack. Other ways to determine an armed attack is to look at intent, presence of declaration of war or kinetic hostilities between the parties to accompany the cyber-attacks. However, in the absence of these or in the absence of information on these factors it is still possible to look at a cyber-attack as an armed attack which differs from conventional land, air, sea, or nuclear attacks solely by the dimension in which it is committed (as recognized at the Wales summit). In this case the judicial opinion of the International Court of Justice should be referenced which defines the “scale and effects” by the merit of which an act is defined as an armed attack” (Karasov, 2018, p. 61.).

The UN Charter prohibits threat of use of force, use of force and aggression except in self-defense. Article 2 paragraph 4 of the UN Charter proclaims, “All members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” Furthermore, it does not prohibit any regional arrangements established
for the purpose of self-defense, such as NATO (UN Charter Chapter VII and VIII). Later on, in the ‘Definition of Aggression’ annexed to General Assembly resolution 3314 (XXIX) Article 3, paragraph (g) use of force and aggression are conveyed as “the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to” an actual armed attack conducted by regular forces, “or its substantial involvement therein”. I have to draw attention to the presence of a “sending state”, therefore in order to define aggression and engage in self-defense there must be an act of attribution. Apart from cyber-attacks not being included in the framework of international law on self-defense the problem of attribution emerges, even more so in the case of cyber-attacks as tracing back the original aggressor with utmost certainty is indispensable but almost impossible. Specifically, in the most recent Ukrainian case of 2014 the “Russian government will likely continue its practice of distancing itself from the Russian nationalistic hacker community thus gaining deniability while passively supporting and enjoying the strategic benefits of their actions” (Carr, 2008, p. 3). If a cyber-attack cannot be traced back to the Russian government than it cannot be classified as an armed attack as the UN Charter and all other legislation building on it is valid in the context of interstate relations. Indeed, although it is an unrealistic scenario, it would be interesting to see what would happen if states could be held accountable for cybercrimes of their civilian population. The Definition of Aggression was elaborated on because the Article 2, paragraph 4, of the UN Charter which defines aggression was too broad therefore, the General Assembly has decided to aid the Security Council in its decision-making process regarding the matter by drafting a definition that gives more guidance. UNGA resolutions are non-binding but this one has been elevated to the level of international customary law by the International Court of Justice. Quoting the UNGA resolution 3314 the ICJ delivered a judgement on the ‘Case concerning military and paramilitary activities in and against Nicaragua’ in 1986 as the United States has - contrary to international law - intervened in the internal affairs of Nicaragua by supporting the opposition in its fight against a leftist government. In paragraph 195 the Court expands upon what is considered aggression. It states „The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces. But the Court does not believe that the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a
threat or use of force, or amount to intervention in the internal or external affairs of other States.” Although a judgement from 1986 could not have possibly included cyber-attacks explicitly mentioned, nevertheless it is obvious that the Court is implying that apart from directly sending conventional armed forces, other acts that are of substantial scale and effects also constitute an armed attack.

The question remains however: how to determine the specifics of the scale and effects? What scale and effects must a cyber-attack have to be classified as an armed attack?

There are several views regarding the question. The first one, advocates that there must be loss of life and material damage involved. However, there are cases when cyber-attacks cause profound damage without the above-mentioned effects. Take the previously introduced Ukraine case of 2014. State websites became unavailable giving the impression to the population that the state functions are impaired. In another scenario where for example the banking and financial sector is targeted by cyber-attacks investors and companies can lose substantial amounts of money. Such an incident could negatively effect the broader economy especially if it happens habitually. Karasov has brilliantly grasped the situation by writing “It appears disproportionate that these cyberattacks would not reach the threshold of armed attack, while their effects may be more severe, long lasting and on a greater scale than other effects caused by traditional armed attacks.” (Karasov, 2018, p. 62).

There is a view, also presented by Karasov, that cyber-attacks should be evaluated from the point of view of their targets – irrespective of their effects and scale. He emphasizes that if a cyber-attack is directed against Critical Infrastructure or Critical Information Infrastructure (which is vital for the operation of Critical Infrastructure) then it can be considered as an attack against the state functions necessary for preservation of territorial integrity, political independence and societal stability and is therefore has the same weight as an armed attack. Such CI and CII can be military installations, platforms for weapons systems and for vital services like the emergency services and air traffic control (Karasov, 2018, p. 61).

Whichever view or a combination of those we chose to consider valid it is without a doubt that cyber-attacks can and do cause damage on a scale of an “armed attack” and therefore have to be included among the triggers for self-defense, among them collective self-defense in the framework of NATO. The damage of a cyber-attack always has multiple layers. The primary effects always target the information system itself and causes its malfunctioning. Loss or theft of data from the system, damage to the hardware can be categorized as such. The secondary effects are those inflicted on the infrastructure operated by the IT system under attack. For example, an incapacitated healthcare database can result in a forced pause of services
in a hospital. Finally, the tertiary effects concern those who would have utilized the services of that infrastructure or system, in our imaginary case the patients. In the case of the 2014 Ukrainian cyber-attacks many consumers had to suffer from power shortages due to the disconnection of the electricity power plant (Karasov, 2018, p. 63).

Although, as I have repeatedly stated, there is no legally binding document on the matter and the decision is made on a political level, nevertheless there is a frequently quoted document going into more detail and probably in practice providing guidance to decision-makers. The Tallinn Manual has been constructed by the CCD COE, a cybersecurity research institute accredited by NATO. The updated version, the Tallinn Manual 2.0, is currently the most comprehensive guide on how international law applies to cyberspace incidents (Matallana, 2017, p. 12). It is a document that could be a good model for national and NATO legislation and norms on cyber security.

The Tallinn Manual despite its progressive nature does not satisfy the normative arguments as it integrates cyber actions in the traditional framework of war. One of the dangers of this is the deterrence aspect. Deterrence against security threats is one of NATO’s founding principles (Article 5). Experts and policy makers have drawn the analogy between nuclear weapons and cyber-attacks, (Spiegel, 2017, p. 47) but they are very different. Nuclear attacks cause only death while the destruction of a cyber-attack can be regulated from annoyance to death, as well as it differs by its vast availability to private actors and difficulty to trace back the aggressor. In case of a nuclear attack it is always known who committed it.

Furthermore, in case civilians are traced back and identified as perpetrators will they be considered combatants in the event of an Article 5 invocation (Spiegel, 2017, p. 55)?

Even the Tallinn Manual does not explicitly state that cyber-attacks are armed attacks. The expert creators of the Tallinn manual stated that while international law is applicable to cyber warfare and identified the Stuxnet case (created by the most powerful Member State of the UN, the USA) as an “act of force”, they did not clarify whether it also qualifies as an “armed attack” (Spiegel, 2017, p. 61). This is what happens if we let political force decide instead of the system of rule of law and sovereign equality of all states.

According to the 2012 Cyber Defense Policy an attack which includes a cyber component is of “political nature therefore decisions lie with the leaders of NATO and the member states, not with the commanders of the reaction forces” (Szentgáli, 2013, p. 88).

Additionally, in case of a cyber-attack states many times opt to settle the matter without using the military or invoking collective self-defense clauses. Alternative methods include: diplomacy, economic sanctions, legal prosecution (for example at the ICJ or other regional...
courts) and cyber retaliation (Ghavaml, 2016, p. 26). In practice, NATO usually responds with buildup of resilience, reparation of damages (defensive means) or by sending a Rapid Reaction Team (RRT) or a unit from the NATO Communications and Information Systems (CIS) Group to assist the targeted Member State or the NATO’s system (Ghavaml, 2016, p. 30). In terms of a possible major cyber-attack against NATO the NAC is likely to decide to invoke Article 5 if (1) the cyber-attack targets the availability or integrity of IT systems in contrast to when it targets confidentiality (data theft, blackmail) (2) the cyber-attack reaches the threshold of an armed attack (scale and effects) (3) clear attribution is possible (4) the aggressor is a state or terrorist organization (Ghavaml, 2016, p. 32).

Reasons for why there isn’t a legally binding document to invoke Article 5 in cases of cyber-attacks are the following:

1. Deliberate decision on the part of the Member States to maintain flexibility due to political reluctance (Afghanistan experience with WMD), lack of willingness to share capabilities or dedicate budget, and in fear of overstretch of NATO beyond its mandate and capability.

2. Diverging views make an agreement impossible as some members might not view countering cyber threats as crucial vis-à-vis other challenges.

3. The NATO organizational structure. NATO’s bureaucracy and decision-making bodies are “too big, too slow” (streamlining would be a great solution), nevertheless in this case the process might be underway it is just very gradual (Tosbotn, 2016, pp. 23-24).
7. Russia’s influence campaign targeting the 2016 US presidential election and the Trump-Russia affair

There was a lot of controversy surrounding the 2016 presidential race. Firstly, this election received exceptional attention from the whole world because the United States is still a preeminent country in the current international arena despite the rise of China. China’s rise meant “merely” the narrowing of the gap between it and the United States. Therefore, the top decisionmakers of the US influence the whole world with their actions. Secondly, the fact that a candidate like Trump (not a politician, started as an independent candidate, infamously went bankrupt before) got so far in the elections as well as his rhetoric were shocking to many around the world, including United States citizens.

Trump has won the elections ultimately however with a narrow margin and only because of the electoral system in the US as taking the total number of individual votes he would not have had a majority! In the United States districts vote for candidates so in this case the districts can be drawn as to favor one or the other candidate (gerrymandering). If this would not have been controversial enough, the whole campaign was plagued by scandals. Many of these resulted from Trump’s overly simplistic, sometimes xenophobic, homophobic and sexist expressions. He won the race in a way due the fact that not enough people voted for his counterpart, Hillary Clinton. The candidate of the Democrat party however well-known her person was or how inclusive and positive was the message she tried to communicate to the electorate lost the race partly due to the fact that she was involved in numerous scandals as well. The biggest of these was caused by leaked emails. The emails have been stolen from hacked email accounts of Democratic National Committee officials and published on DCLeaks and Wikileaks.

The emails contained proof of the DNC’s interaction with a biased journalist who gave unfair advantage to Hillary in the presidential debate, several high ranking officials of the DNC expressing their favoritism of Clinton vis-à-vis Bernie Sanders in the primary and information about the identity of financial contributors (WikiLeaks: Hillary Clinton...).

Two reports by the American state were released in the end of 2016/beginning of 2017 explicitly stating that the hacking was conducted by Russian hackers, that they were instructed by Vladimir Putin Russian president, and that they did it with the goal to decrease Hillary’s chances in the race vis-à-vis Trump (DHS and FBI, 2016; CIA, NSA and FBI, 2017). These reports however did not make assumptions about how successful this attempt was or in other words would Hillary have won the election if not for this scandal.
The Joint Analysis Report from 2016 compiled by the US Department of Homeland Security and the Federal Investigation Bureau describes the phenomenon as part of a two year process they codenames Grizzly Steppe in the course of which RIS (Russian civilian and military intelligence) compromised systems of critical organizations and leaked info to the public and the press. One hacker group described by the DHS and the FBI codenamed APT29 started its operations from the summer of 2015 when they broke into systems of critical organizations from political parties to schools and established remote control. Another group codenamed APT28 used phishing to gain access operating from spring of 2016. The report describes a long list of other RIS under names like CloudDuke and SYNful Knock that have been intervening with American systems. The report has been created for network operators and systems administrators to provide them with security strategies recommended to mitigate further vulnerabilities (DHS and FBI, 2016).

In the second report released in the beginning of 2017 the CIA, FBI and NSA detail their assessment about Russia’s influence campaign targeting the 2016 US Presidential Elections. The Intelligence Community Assessment highlights that it is compiled based on often incomplete information and logic not facts. The authors clearly distinguish between information and their own judgements and apply other “tradecraft standards” described in the beginning of the report to ensure accuracy. Estimative language is used to express judgement about the likelihood of an event and confidence in the credibility of the sources. The attribution of the cyber operations was in great part based on existing knowledge. The report concentrates on political nature of the hackings and only the declassified version of the original report is available publicly to avoid exposing certain sources of information. The key judgements of the report are as follows. Vladimir Putin, President of the Russian Federation ordered the operation in 2016 to discredit American democracy on one hand and candidate Hillary Clinton specifically on the other hand. Putin wanted to make the US look hypocritical in retaliation for the Panama papers\(^4\) and the Olympic doping scandal\(^5\). The latter assessment is further confirmed by leaks of WADA (World Anti-Doping Agency) documents which have probably also been committed by GRU. GRU is the biggest Russian foreign military intelligence agency of the General Staff of the Armed Forces directly reporting to the minister of defense and the

\(^4\) A scandal caused by leaks from a Panamanian law firm specializing in offshore companies. Putin has been revealed to have been laundering billions this way among many other powerful and famous clients (International Consortium of Investigative Journalists, 2016).

\(^5\) Russian athletes have been banned by WADA from participating in the 2016 Rio Olympics and the 2018 PyeongChang Winter Paralympics due to a state-run doping program for the London 2012 Olympics and the Sochi Winter Olympics in 2014 (The Guardian, 2019).
Chief of the General Staff unlike other intelligence agencies which report to the president. Therefore, it commands a great number of special forces troops apart from intelligence service agents. Putin sought to discredit US to prove that it has no moral right to criticize Russia.

Furthermore, Putin developed a clear preference for Trump because of his more Russian-friendly attitude in Ukraine and Syria which made an anti-ISIL coalition more likely. He also evaluated Trump as more lenient towards Russia due to his business interests as other country leaders are like Berlusconi. On the other hand, Putin personally hated Clinton for publicly inciting mass protests against him in 2011-2012 and her comment towards him. He sought to discredit her to harm her electability and her credibility during her presidency. Clinton had an aggressive anti-Russia rhetoric during her campaign. In the wake of Clinton’s anticipated victory state funded media, 3rd party intermediaries and paid social media users (“trolls”) prepared a #DemocracyRIP campaign on Twitter which was called-off following Trump’s surprising victory. The same “troll” accounts that supported Ukrainian intervention of Russia started to advocate for Trump even before his election.

The hackers gathered information about organizations that are likely to shape future US policies. The gained access to DNC (Democratic National Committee, the governing body of the United States' Democratic Party) networks from 2015 July to 2016 June. Furthermore, information from the compromised email accounts of Democratic Party officials was leaked through the hacker Guccifer 2.0 (who was likely a group of hackers from the Russian intelligence) on DCLeaks and Wikileaks. Russia Today was made the only Russian media outlet to have access to Wikileaks. Russian media aimed at English speakers like RT America (Russia Today franchise) and Sputnik gave negative coverage to Clinton and positive to Trump claiming that Trump is unfairly treated by the US media due to his lack of connections to the corrupt deep-state dominated by corporations.

The hackers also compromised the Republican party’s system, but they decided not to reveal any possibly stolen information.

In conclusion, the Intelligence Services agreed that Moscow will continue to exert its influence worldwide and will likely use lessons learnt from 2016 to meddle with elections in Europe. The report states that Russia combines overt (propaganda) and covert (cyber) intelligence operations and enjoys maintaining deniability. These mixed techniques had also been demonstrated in Ukrainian 2014. Putin has denied Russian involvement but said it was important to disclose the DNC information to the public (CIA, NSA and FBI, 2017).

These reports reveal that the Republican party’s system was also compromised therefore it is possible that the hackers have obtained sensitive information about Trump’s business and
private life and used it to blackmail the to-be-president. Logically, if the Russians conducted such a controversial operation, they must have had some serious reason for it. The risk of being discovered and traced back was very high, even though proving a cyber-attack is always more difficult than a kinetic one. The consequence of this for the already terrible reputation of Russia on the international scene could have been far graver. Knowing this and still taking the risk suggests that there is some hidden or long-term benefit for Russia from Trump’s victory. That is if we evaluate the situation from a realist “potential gain vs. risk” standpoint. The Russian economy has never performed marvelously after the regime change in the 90s but as a consequence of the sanctions imposed on it as a punishment for their Ukrainian involvement it became even more isolated and just generally characterized by negative tendencies. Could the Russian leadership possibly hope for an improvement of relationship with the USA if Trump is the president? In his election campaign Trump was certainly friendlier in his discourse towards Russia compared to Clinton. On the other hand, even during his campaign, Trump has showcased that he is unpredictable or rather unreliable. Firstly, he lacks knowledge and experience in the field of politics, diplomacy, international affairs and leadership in general (being a leader does not equal being a boss). Secondly, Trump’s personality in itself makes him a weak link because he is very impulsive, known to be unable to listen to advise and to regard the States as a business enterprise where profit is the goal and whose assets can be risked in a lucrative but volatile environment. Country leaders like to know how their countries stand vis-à-vis each other and change of this status quo is the biggest risk for emergence of conflict in the international arena and not domination by a hegemon. Therefore, with Trump, when every day his approach changes about certain issues and actors, USA risks becoming an entity that the other countries would prefer not to be involved with whatever the situation may be. Real life shows even many allies seem to be shunning the US nowadays (for example Canada). It is questionable whether the Russian leadership would prefer to deal with the USA with Trump in the White House. An important detail to mention is that Russia has engaged in other, seemingly illogical, foreign policy activity in the past. There are many “frozen” conflicts at its borders, all on the territory of the former Soviet Union, probably a land Moscow considers to be its exclusive sphere of interest. These are South Ossetia and Abkhazia of Georgia, Transnistria of Moldova, Artsakh of Azerbaijan, and most recently Donetsk and Luhansk regions of Ukraine. These separatist strifes are all – even though unofficially – supported by Russian forces. This activity takes a toll on the Russian budget, money that could be spent elsewhere. Moreover, these disputed territories are a cause of constant confrontation on the international forums, a
source of sanctions rather than a means to be used as bargaining chips. Regardless, Russia seems to be keen on maintaining these conflicts, seemingly motivated by national pride.

It is important to mention that it is very difficult to prove that the Russians did the hacking or the connection between the hacker group and the Russian president. Many other actors have tried to hack American targets before and the USA itself hasn’t shied away from influencing internal politics of other “sovereign” states - with more of less success. Following the two reports mentioned above, Trump have also officially admitted that the hacking was committed by the Russians but the evidence of the connection between the hackers and Putin is contained in the classified section of the report – if it’s there at all. However, if this could happen in the United States other countries are rightfully worried about similar interventions into their internal political life, their national elections.

However, not only Russian propaganda-channeling media and Trump (previously) denied Russian involvement. IT experts criticize the two American reports because it is virtually never possible to identify who is exactly behind cyberattacks personally. There are only tools of cyberwarfare (programs, computers, networks) which have been used previously in other cyberattacks which have also been traced back to “Russia”. The tools used in the hacking of the Democrat party’s system characterize a Russian hacking group but has been proven to also be in the hands of Ukrainian hackers, a cybersecurity company called ESET and other actors could also have it. Additionally, the identification of these tools was suspiciously simple as the hackers left behind very obvious traces that lead back to Russia, almost as if it was done on purpose. Lastly, the FBI that composed these reports have not even looked at the servers of the Democratic Party but relied on information provided by a private company, CrowdStrike that was hired by the Democratic Party itself (index.hu Az évtized...).

FBI has first initiated investigations after Australian officials disclosed that George Papadopoulos, a Trump presidential campaign adviser, had told Alexander Downer, the Australian High Commissioner to Britain over a dinner with alcohol that the Russians have hacked Hillary. The public first gained knowledge about the allegations that Russia meddled with the elections from a joint statement made by the two top Democrats on the Senate and House Intelligence Committees. Later the Intelligence Community confirmed the allegations. Furthermore, another document has been revealed to be affirming accusations both about Russian involvement and cooperation with the Russians by the Trump campaign. Called the Trump-Russia dossier, the document has been compiled by a former MI6 (British intelligence) officer Christopher Steele. The report has been ordered by a private company Fusion GPS and paid for firstly, by the Republican National Committee, then the DNC and Hillary’s campaign,
and lastly handed to the FBI when funding by the political parties ceased (Christopher Steele's report...). The FBI regarded the Steele dossier as a trustable source even though the fresher Mueller report has denied its major claims. After taking over the White House from Barack Obama, now former President of the United States, Trump has fired FBI director leading the investigation in the case up to that point. After protests by Democratic representatives Robert Muller was appointed the head of the investigations as Special Counsel. The Special Counsel operates independently from the Attorney General, submits his findings to the Attorney General who then relays information to the Congress. The Mueller report investigates whether Trump’s campaign members had ties with Moscow and whether Trump has tried to obstruct the investigation. One of the individuals investigated is Michael Cohen, the President’s former personal lawyer (Mueller, 2019).

Former DNC chair, now Democratic Representative Wasserman-Schultz questioned Michael Cohen on the WikiLeak email dump on February 27, 2019 in a House Oversight Committee hearing. Cohen stated that Trump would do anything and collaborate with anybody to win the elections. He further claimed that Trump and his family had business interests in Russia worth hundreds of millions of dollars however he has no knowledge about whether the Trump family was compromised by any foreign entity. Additionally, Cohen declared that Trump’s campaign never expected to win the elections and it was only an opportunity to promote himself for business and accused the now-president of financial fraud partly for tax evasion. Cohen disclosed that Roger Stone, who provided information to Trump „for free‟, was not authorized by Trump but his contributions were very welcome. Stone, who is described as an informal advisor to Trump, had allegedly made contact with Wikileaks founder, Julien Assange (now arrested) prior to the email dump and had notified the Republican candidate about the leaks. Currently, Stone insists that he previously lied about meeting Assange and his goal was to provoke the Democratic party. The Mueller Report confirms this. Nevertheless, Cohen, could not provide information on whether Trump had paid hackers or collaborated with the Russians in that regard or knew about the hacking prior to just before the emails were going to be released (PBS NewsHour: WATCH: Former DNC chair…). The Mueller Report reveals that Cohen lied to the Congress about Trump’s business interests in Moscow (Trump tower) and Trump did not ask him to do so. In fact, despite Cohen’s attempt to gather Russian support in building a Trump tower in Moscow his requests were rejected. Moreover, Trump didn’t know about the leaks in prior to the Wikileaks release.

Mueller’s findings have been presented in a report (the full version is not public). The report states that Trump has not collaborated or conspired with the Russians however he did
make a considerable effort to impede the investigation. Now the Congress and the Senate have to deliberate on his impeachment. It is unlikely to happen as the 2020 elections are nearing because it is not worth for the Democratic party to waste its efforts to impeach Trump for impeding an investigation on a conspiracy that didn’t happen. The main reason contrasting this view is that examples of impunity are likely to breed more lawlessness. Others suspected of having connection to the DNC leak case are: Trump campaign aide George Papadopoulos, foreign policy adviser in Donald Trump's 2016 Presidential campaign Carter Page, National Security Adviser Michael Flynn, Donald Trump Jr., Senior Advisor to the President of the United States Jared Kushner (and Trump’s son-in-law), Trump campaign chair Paul Manafort, and Attorney General William Barr. The report identifies that some of them indeed had common acquaintances with the Russian government and impeded the investigations but does not indict any of them for conspiring with Russia to influence the election in 2016 (Mueller, 2019).
8. Implications of the Trump-Russia case for NATO Article 5

NATO declared in its Wales Summit Communiqué in 2014 that International Law would apply in cyberspace. However, it classifies cyber threats as “non-conventional” and declares that invocation of Article 5 in the event of a cyber-attack would be decided on a case-by-case basis (Allison, 2018). These announcements seem to be in a slight contradiction with each other. But will these statements suffice? They are broad and allow for much needed practical flexibility. But at the same time the Trump case shows that for effective deterrence there is a need for stricter regulation.

Estonia didn’t invoke Article 5, while Georgia and Ukraine aren’t NATO members however now with the Trump case it is important to rethink the question. Should the intervention of Russian hackers into the course of the US presidential elections be considered a breach against the political independence of the States? Yes, it can be as they could have potentially changed the outcome as the difference between the two candidates was marginal. “A cyber-attack that releases sensitive information on a presidential candidate could influence the results of a ballot decision, corrupt the institutional integrity of nationally held elections, and even prompt regime change” (Ghavaml, 2016, p. 2). Consequently, depending on our interpretation, it can be qualified as to have caused damage equivalent to an armed attack because it has prevented the state from carrying out its functions. In order not to engage in speculation it is absolutely necessary to provide a solid legal background for cyberattacks in the light of the Trump-Russia case. It is obvious why political decision making will not work here. The United States, in order to invoke Article 5, has to pronounce that it has been a target of “armed attack” or “aggression”. Other states cannot decide to “help” the US and instruct NATO to investigate the case. However, with Trump being the president of the United States, the US will never call for Article 4 or 5 in this particular case. This case is an excellent illustration as to why it is necessary to create a legal mechanism for investigation of, defense and deterrence against cyber-attacks without the need of political deliberation first. It is essential to ensure equal treatment (sovereign equality) and rule of law.
9. Conclusion

The problems are legal and normative. If legal: exactly how to determine if a cyber-attack is classified as an armed attack? What should be the threshold? If technical: who attacked? It’s difficult to trace back. Should the state take responsibility? That leads to another normative problem: states would securitize the cyber domain and take away our freedom to avoid being held accountable for actions of their citizens or actions committed on their territory. It has the potential to create a myriad of police states and would probably make the world unlivable. History teaches us the lesson that people want freedom and have continuously strived to achieve it. Therefore, creation of police states would lead to increased violence – quite a counteractive measure.

The Trump-Russia affair have signaled the onset of an era when using capabilities from the cyber domain (hacking and misinformation campaign) is sufficient to change the course of political events - even in the US, the stronghold of liberal democracy. Based on the current information available – the latest being the Mueller probe – Trump has not colluded or conspired with the Russian hackers. Despite this, “Russiagate”, as the scandal is often referred to in the media, has taken up half of Trump’s presidency and is likely to continue. The public and Congress members accuse the Attorney General of misinterpreting the report on purpose and presenting its findings in a lenient light. This scandal has in big part distracted the public opinion from other crucial issues Trump is failing to deliver on. The biggest harm was not inflicted on Hillary who lost the campaign, nor Trump who was discredited in the eyes of the electorate but on the credibility of the US democracy. It truly showcased the ruthless and corrupt nature of top politicians and electoral campaigns. Imagine a case where a country with far less checks and balances in its political system is targeted with the same means. The consequences could be catastrophic. One way to shield smaller, less developed countries could be the creation of an umbrella against cyber intrusions on the political and technical level. One without the other would mean the failure to capitalize the existing organizational structure of NATO and its long past of successful partnership.

The Trump case perfectly showcases why the current setup on invocation of Article 5 is not sufficient. There is a need for a legally binding document that pronounces cyber-attacks to be of equivalent weight to kinetic attacks when it comes to collective self-defense, among other means by the invocation of Article 5. Apart from its practical necessity such a strong framework would be of indicative use as well, and a framework for an emerging field of International Relations, cyber diplomacy to rely on.
In the future NATO is recommended to take a comprehensive approach. First off, it should maintain its land forces as it has always proven to be a good way to deter potential aggressors. Concentrating on cyber defense should not deter the organization from maintaining conventional land forces. Secondly, for the survival of NATO it is imperative that the key decision-makers recognize the changing security environment and make NATO adapt to it. This includes further investment into and greater attention to cybersecurity. Thirdly, to allow these changes and constants manifest, and to create an efficient and stable organization that can continue to reassure its Members about the power of its collective it is essential to reinforce solidarity in the form of defense spending, set at 2% (Matallana, 2017, p. 15).

All the above-mentioned recommendations are necessary if NATO wants to remain the guarantor of Transatlantic security, stability and prosperity.
Annex I. 2016 Presidential Election – Who won the popular vote?

<table>
<thead>
<tr>
<th>Candidate</th>
<th>Party</th>
<th>Electoral Votes</th>
<th>Popular Votes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Donald J. Trump</td>
<td>Republican</td>
<td>304</td>
<td>62,980,160</td>
</tr>
<tr>
<td>Hillary R. Clinton</td>
<td>Democratic</td>
<td>227</td>
<td>65,845,063</td>
</tr>
<tr>
<td>Gary Johnson</td>
<td>Libertarian</td>
<td>0</td>
<td>4,488,931</td>
</tr>
<tr>
<td>Jill Stein</td>
<td>Green</td>
<td>0</td>
<td>1,457,050</td>
</tr>
<tr>
<td>Evan McMullin</td>
<td>Independent</td>
<td>0</td>
<td>728,830</td>
</tr>
</tbody>
</table>

(wikipedia)
Bibliography

I. Primary sources:

2011. évi CXII. Törvény az információs önrendelkezési jogról és az információszabadságról
http://njt.hu/cgi_bin/njt_doc.cgi?docid=139257.338504

Charter of the United Nations. San Francisco, California. 26 June 1945

Christopher Steele's report published by Buzzfeed
https://www.documentcloud.org/documents/3259984-Trump-Intelligence-Allegations.html

CIA, NSA and FBI: Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution (declassified version of a highly classified assessment). 2017.01.06.


PBS NewsHour: WATCH: Former DNC chair Wasserman-Schultz questions Michael Cohen on WikiLeaks email dump https://www.youtube.com/watch?v=qIFUcuJ4Q4k


II. Secondary sources:

Allison, George: NATO working on cyber attack trigger for Article 5. 19 March 2018


Healey, Jason and Leendert van Bochoven (February 2012): NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow. Issue brief as part of the Atlantic Council’s Smarter Alliance Initiative.


Kramer, Franklin D., Robert J. Butler, and Catherine Lotrionte (2016): Cyber, Extended Deterrence, and NATO. Issue brief for the Atlantic Council

Luukas K. Ilves, Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau (July 2016): European Union and NATO Global Cybersecurity Challenges: A Way Forward. PRISM Vol. 6, no. 2


Shea, Jamie (2010): *Why does NATO’s new Strategic Concept matter?*


**III. Other sources:**

bbc.com *Facebook data: How it was used by Cambridge Analytica*  


index.hu *Biden megerősítette, hogy Obamával látták a Trumpról szóló állításokat*  

index.hu *Az évtized botrányává dagad az orosz hekkerügy*  

index.hu *Európa felkészül a kiberháborúra*  
index.hu Javában zajlik a kiberháború Oroszországgal
https://index.hu/velemeny/2016/07/05/javaban_zajlik_a_kiberhaboru_oroszorszaggal/
Accessed 2019.01.19.

index.hu: Nemcsak adatokat, éleket is veszíthetünk
https://index.hu/tech/2016/01/20/nemcsak_adatokat_eleket_is_veszithetunk/ Accessed 2019.01.17.


Johnston, Anna (April 19, 2015): Bradley Cooper’s taxi ride: a lesson in privacy risk

Kaspersky Lab: What is a Botnet? https://www.youtube.com/watch?v=3BbxUCOFX8g
Accessed 2019.01.17.

Kaspersky Lab: What is a DDoS Attack?
https://www.youtube.com/watch?v=yLbC7G71IyE&list=PLPmbqO785Hlu-lW7655fc7XxzjGBSdiut Accessed 2019.01.17.

NATO Cooperative Cyber Defence Centre of Excellence website

Nemzeti Kibervédelmi Intézet (NKI) website http://www.cert-hungary.hu/

No More Ransom! initiative by the Dutch police, Interpol and McAfee

The Guardian (February 2019): Russia doping scandal.
https://www.theguardian.com/sport/russia-doping-scandal