Can a Cyberattack Become an Act of War? European and Trans-Atlantic Perspectives

Sorin Ducaru, Mihail Caradaică, Ana Maria Costea[1]

***Abstract**: In the last two decades, along with the process of digitalisation of businesses and state apparatuses, the world has faced a new major issue that can produce physical / non-physical damage, and equally threaten individual security and the state's sovereignty: cyberattacks. Confronted with the strategic competition – within a multipolar world – coupled with this new challenge that can redefine the nature of war, NATO member states have tried to find a common answer by linking cyberattacks to Article 5 of the Washington Treaty, NATO's collective defence principle. Understandably, Article 5 was drafted while having in mind the aspects of deterrence and defence related to conventional wars. However, it has been invoked by the Allies only once, i.e., after the 9/11 terrorist attacks against the USA, which represented quite an unconventional scenario, certainly unanticipated by the Alliance's Founding Fathers. Given the current trend, and reflecting on the increase in the complexity, intensity and persistence of the known cyberattacks, it is important to study the potential game-changing circumstances of such unconventional attacks, which might trigger Article 5 and its collective defence principle. The present paper seeks to depict the complexities and consequences of cyberattacks within the framework of the collective defence principle.*

***Keywords**: Article 5, cybersecurity strategies, cyberwar, deterrence, NATO.*

Introduction

Today, cybersecurity has become one of the most debated issues in the field of strategic studies (Caruson, MacManus and McPhee, 2012) due to the increasing attention given to it by media, decision-makers, representatives of private companies, scholars, and the wider public. As our private lives, the economy, state apparatuses or democratic processes went online during the COVID-19 crisis (the pandemic speeding up this process already underway), cyberattacks have increased by 600% (PurpleSec, 2021), thus becoming one of the top issues on the political agenda of the West. Additionally, they have become more sophisticated in a world with no physical borders, where the technological development constantly changes the security framework and creates a security void. The accelerated infrastructure transformation of the digital technologies entails vulnerabilities and cyber threats, which may cause huge economic losses for private companies, leakage of national sensitive information or of a huge

[1] **Amb. Sorin Dumitru Ducaru** is the Director of the European Union Satellite Centre (SatCen) since June 2019. E-mail: sorin.ducaru@satcen.europa.eu.
Mihail Caradaică is Lecturer at the National University of Political Studies and Public Administration (SNSPA), Department of International Relations and European Integration in Bucharest, Romania.
E-mail: mihai.caradaica@dri.snspa.ro.
Ana Maria Costea is Associate Professor at the National University of Political Studies and Public Administration (SNSPA), Department of International Relations and European Integration in Bucharest, Romania.
E-mail: anamaria.costea@dri.snspa.ro.

amount of private data, and physical disruption of critical infrastructure that can affect the national security of a state. In the following paragraphs, we shall highlight some relevant examples on how cyberattacks impacted both the economy and the society.

Attacks like **WannaCry** (Ehrenfeld, 2017; Mattei, 2017; Volz, 2017), **Stuxnet** (Farwell and Rohozinski, 2011, pg. 23; Fidler, 2011, pg. 56), **SolarWinds** (Jibilian and Canales, 2021; Soliman, Simon, De, Hungerford, Ito, Lev, Nadadur and Silverstein, 2021) and **Heartbleed** (Banks, 2015, pp. 1-2; Jeske, McNeill, Coventry and Briggs, 2017, pg. 174) emphasise how cyberattacks could represent a threat to the economy, privacy, or to the citizens' trust in the democratic systems. According to Watkins, cyberattacks on private entities have generated considerable losses in terms of intellectual property, business flow or business intelligence, and tend to increase the security costs of those companies (Watkins, 2014, pg. 3). Therefore, the private sector is already allocating important resources for organising its defence against cyberattacks. In its turn, the state should be responsible for defending its own citizens, its economy, and critical infrastructure, and thus its security. Global spending on cybersecurity products and services is estimated to have exceeded $1 trillion cumulatively over the five-year period from 2017 to 2021 (Embroker, 2021). Furthermore, as it was demonstrated in several cases (i.e., the Russian war against Georgia in 2008, the illegal annexation of Crimea in 2014, and the invasion of Ukraine in 2022), cyberattacks have become part and parcel of the military planning and the subsequent war actions.

Taking all this into consideration, our aim is to see how NATO would respond to a cyberattack under the umbrella of Article 5. In order to do that, we shall analyse how member states perceive cyber threats, and how they are planning to tackle them at national and international levels. Our research starts by identifying the threats, since this represents the first step in developing any security strategy for both public and private entities. It continues with the analysis of the actors in the cyberspace, and the reasons behind an attack. These elements are quintessential in any current security framework, since the ability to define properly one's opponent is directly linked to the capacity to respond – in an efficient and sustainable strategic way – to his threats.

The topic is of critical importance, as it will be further argued, because cyber has been defined as a domain of military operations, consequentially generating significant changes in military strategic doctrine and planning (including aspects like the application of Article 5, or the rules of engagement related to military planning, etc.). Last but not least, NATO represents one of the most powerful military alliances based on the consensual decision-making process (involving all member states) as well as on the adherence to the principles and norms of international law. NATO proved to be efficient, over the years, due to the high level of interoperability shared by the Allies during their joint military campaigns for all the four common operational domains (land, sea, air, and space). Hence, the harmonisation of perceptions, thresholds and actions was essential in dealing with the 21st century threats. In order to cope with the cyber threats and apply Article 5, the Allies have to share a common view on the threats to be tackled, and the most suitable way to respond to them, just as they do in the other four operational domains. In view of the above, we have conducted qualitative research on the NATO member states' declared national security threats, according to their programmatic national security documents, to see if we can identify a common denominator and if, in fact, Article 5 can be applied in the case of a cyberattack.

1. Research methodology

As previously stated, the aim of this paper is to analyse how NATO would react to a cyberattack, since the cyber domain was included among the operational domains of the Alliance. Hence, the following research questions arise: "Can a cyberattack be considered an act of war?"; "Can NATO trigger Article 5 in the case of a cyberattack, and what are the chances that it will?". In order to answer these questions, the research focuses on several aspects:

Firstly, we shall conduct a specialised literature review by targeting disciplinarily interconnected fields throughout this paper:

- The legal aspects regarding the applicability of Article 5 in case of a cyberattack (the Tallinn Manual's view).
- Aspects of warfare theory: the various definitions of war and how we can apply them to the cyberspace (Carl von Clausewitz, Thomas Rid's and John Stone's diverging points of view, etc.).

Secondly, the paper includes a review of the main NATO developments in the field of cyberspace. This step is necessary to indicate, from a procedural perspective, when a cyberattack could come under the umbrella of collective defence.

Thirdly, to identify a possible common view among NATO members, the paper will analyse the approaches at national level by developing a comparative evaluation of the cybersecurity strategies of all the Allies[2]. The comparison will be made by using different variables like: *actors in cyberspace*, *types of attacks*, and *triggers*.

The actors will be split into two main categories: state and non-state actors. The latter will encompass three types: criminal organisations, terrorist groups, and individuals. This distinction is necessary because the legal framework applicable to each cyberattack differs (in line with international and national law), depending on the attacker. Thus, the application of Article 5 may not be possible in the case of an attack conducted by non-state actors unrelated to a state. The actor type is extremely important since it is directly connected with the very nature of war and how it is waged nowadays. Last but not least, as previously mentioned, the ability to identify the attacker in a proper and realistic way is a must for decision-makers. A failure in this direction will lead – from a strategic point of view – to an inefficient response to the existing security threats.

This element is, also, directly linked to the second element of comparison, namely the types of threats. To be able to develop a security strategy and to defend oneself, one needs to know the threats that ought to be countered. Given the diverse nature of actors involved in the cyberspace, the types of threats identified are the following: cyberattacks, cybercrime, cyber espionage, cyber terrorism, cyber sabotage, information/ cyber warfare and hacktivism. We have deemed this analysis necessary because the application of Article 5 depends on the decision of NATO member states to

[2] In order to do this, we have extracted the relevant information (regarding the actors, the threats, and the reasons) from the cybersecurity strategies of NATO's member states that joined the Alliance before 2023 (Albania 2018; Belgium 2019; Bulgaria 2018; Canada 2018; Croatia 2015; the Czech Republic 2015; Denmark 2018; Estonia 2018; France 2015; Germany 2016; Greece 2018; Hungary 2013; Iceland 2014; Italy 2013; Latvia 2019; Lithuania 2018; Luxembourg 2018; Montenegro 2018; the Netherlands 2018; North Macedonia 2018; Norway 2019; Poland 2019; Portugal 2019; Romania 2013; Slovakia 2015; Slovenia 2016; Spain 2019; Türkiye 2016; UK 2016; US 2018).

treat a cyberattack as an armed attack. Since Article 5 was triggered only once in NATO's history, and there is a huge debate at international level regarding the possibility of a cyberattack reaching (through its scale and effects) the threshold of an armed attack, it is very hard to believe that the Allies will act/react in unity, if they do not see the threats in a similar manner. Here, the harmonisation of perceptions is a leitmotiv if the desideratum is a unitary response.

The third element of comparison is represented by the attackers' reasons or aims. This part is essential for understanding if and how the concepts of war and deterrence are altered by the cyber field, and thus how the strategic level is/should be altered.

As previously mentioned, from a conceptual point of view, the analysis focuses on several theoretical concepts, like "war", "deterrence", and "cybersecurity". The processed documents are National Cybersecurity Strategies, or National Security/ Defence Strategies (if a specific national cybersecurity strategy was not adopted) that include a section dedicated to cyber-defence/security. Regarding the limits of the research, not all national strategies were available in English, but we have overcome this hindrance by translating them into English. Another limitation in the research derives from the fact that not all strategies have been adopted at the same time. Thus, the national and international contexts of their approval may reflect the stance of those countries in a specific moment in time. On the other hand, since no other official document has been released yet, we consider the one available to still reflect the current view of the state.

2. Background

2.1. Literature review

The rapid growth of cyberspace created a new battlefield, and pushed NATO to adapt to new security circumstances and include cyberattacks in the scope of Article 5. This change was seen as a security necessity due to the rather unique feature of cyberspace, able to cause maximum damage at the lowest cost possible, and with a high degree of deniability. This feature was specifically shown during the Estonian attacks in 2007 or during WannaCry, Stuxnet, etc. As Nye Jr. mentions, it is rather cheaper to navigate online across the globe, than to move large military equipment like warships (Nye Jr., 2011, pg. 20). This aspect in particular reveals the huge development opportunities for the cyberspace, but also poses an important threat to the national and international security. Coupled with the diversity of actors and motives that will be further analysed, it can turn cyberspace from the most beneficial result of technology to the worst cost that we could pay in terms of security. Before examining the strategies of NATO's Allies and the applicability of Article 5, we need to define first the concepts we are working with. Following the reasoning of Tarja Rusi and Martti Lehto, we shall define the cyber-threat as a malicious act meant to destroy, damage, or disrupt a system or a computer network (Rusi and Lehto, 2017, pg. 323). The cyber-threat usually uses elements like networks, software and computer technology, with the aim of committing a traditionally illegal act (Lester, 2016, pg. 2). Meanwhile, we should bear in mind that **a cyberattack can have both physical** (Stuxnet, and WannaCry that blocked the access to the patients' medical files had a physical impact) **and nonphysical consequences** (the 2007 Estonia attacks, SolarWinds, the attacks against Sony Pictures, etc.). Taking into consideration the relatively low costs and the extent of the extremely varied consequences (which can go till the physical destruction of nuclear power plants), we could say that cyber tools can be counted among the most dangerous assets of society nowadays, after the weapons of mass destruction (WMD). Given the indiscriminate effect of most cyber-tools and attacks, as well as their great propensity to spill over the World Wide Web, it is easy to understand why many analysts compare the effects of malicious cyber-tools with those of WMD, or define them at least as "Weapons of Mass Disruption". What renders cyber-tools possibly more dangerous than chemical or nuclear weapons (for example) is the fact that the latter pertain to a very limited group of states, and both the materials and the know-how (necessary to their production) are extremely limited and subject to a severe non-proliferation regime. It is very difficult to conceal their development, as these military tools are constantly supervised by international bodies, like the Organisation for the Prohibition of Chemical Weapons (OPCW), and the International Energy Agency (IEA), respectively. Conversely, in the case of cyber weapons, the actors vary from states to non-state players, like groups of hackers, individual hackers, terrorist organisations, organised crime, etc. With this variety of actors comes a variety of motives standing behind a cyberattack: from rational, and therefore predictable, motives to irrational, thus unpredictable behaviour. Last but not least, in terms of quantifiable results we have already seen the consequences of an atomic bomb with Hiroshima and Nagasaki, but the same cannot be said regarding cyberwar. From the aforementioned point of view, we could arguably state that, after chemical and nuclear weapons, cyberattacks are among the most dangerous tools in terms of potential impact (if an attack is so large that it cuts off the electric power grid of major cities for a large period of time), considering that we still do not know how an ultimate cyber weapon would look like. Last but not least, cyber weapons are impossible to define or standardise in terms of "calibre" or "TNT kilotons" equivalent. The main aspect, which could be used to differentiate between the various cyber-weapons or attacks, remains the severity of their impact and this, unfortunately, is a *post factum* approach.

If we bring the discussion into the area of strategic studies, we cannot properly highlight the features and the character of the new wars without strong references to Carl von Clausewitz. He defined war as a duel on a larger scale or as an act of force meant to impose a certain will of the winner upon the loser. For him war represents a paradoxical trinity, which comprises primordial violence, hatred, and enmity (Clausewitz, 2017, pg. 30). In the end, "*war is nothing but the continuation of politics with other means*" (Clausewitz, 2017, pg. 30). This definition raises several debates when referring to a cyberwar.

Firstly, in terms of actors, in the cyberspace we have a variety of players, both state and non-state actors. From the state-centric point of view, this definition applies irrespective of the tools developed and used during a war. Yet, the cyber arena is not only the playground of states. Non-state actors can generate disturbance/destruction for fame/international status or political/economic purposes. Each particular group has its own agenda, its own motives, which may not have anything to do with either political gains, or economic ones. At the same time, for the attack to be considered an act of war, a state should be responsible for the actions of the non-state player, as the international law specifies with regard to the principles of international responsibility. This raises the issue of attribution, which is in itself a problem in the cyberspace. However, we can reasonably say that the activity of an individual conducting malicious cyberattacks to gain international status cannot be labelled an act of war, at least not in the view of international law.

Secondly, as Clausewitz mentioned, war represents a paradoxical trinity. From this perspective, Thomas Rid (2011) considers that a cyber-offensive act may be deemed an act of war, if it is *"violent, instrumental and political"* (Rid, 2011, pg. 2). According to him, no single cyberattack has yet met all the three criteria (Rid, 2011, pp. 10-15). He argues that one should distinguish between acts of war, sabotage, espionage, and subversion activities. From this angle, Stuxnet should be considered an act of sabotage, since it lacks violence and political attribution (Rid, 2011, pp. 16-20). At the same time, John Stone thinks that acts of sabotage can be considered acts of war, since the concealment of the political goals is part of the strategic framework of war. Furthermore, wars do not necessarily employ high degrees of violence, especially if the attacker has the technological means to avoid it. Thus, cyberattacks ought to be viewed as *"particularly efficient means of translating force into violence"* (Stone, 2012, pg. 107). Last but not least, in his opinion, Clausewitz's definition refers to physical force, not to violence. Another distinction between cyberattacks is provided by the targets. In the case of acts of war, the targets are humans, whereas in the case of sabotage the targets are economic/military non-human objectives. Nevertheless, as Stone underlines, we cannot always make a clear distinction between an act of sabotage and an act of war (Stone, 2012, pp. 103-106). Hence, returning to the case of Stuxnet and applying Clausewitz's definition, we could say that:

- It was a politically targeted attack aiming to heavily affect the Iranian nuclear programme, and thus instrumental.
- It employed force (Foltz, 2012) to cause damage to a military objective of strategic military value for the opponent, with the ultimate aim to make Iran behave in a certain desired way.

Also, if we apply Stone's view of the war as an act of force (not necessarily violence), which *"does not require the act to be claimed or attributable"* (Stone, 2012, pg. 105), we could argue that Stuxnet represents the best-known cyberattack that got the closest to being considered an act of war. Therefore, it could have triggered a retaliatory response, namely cyber-war actions.

Another scholar that defined the cyberwar is Joseph S. Nye Jr., who considers that *"a more useful definition of cyber-war is, hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence"* (Nye Jr., 2011, pg. 20). Thereby, even if it is a bloodless form of violence, it could create large physical destruction and billions of dollars in damage. Thus, in order to reach the level of a cyberwar, the conflict can have a virtual layer, but the impact should be physical in its nature (McGraw, 2013), criteria that were met in Stuxnet's case.

From a practical point of view, NATO has tried to tackle the emerging threats in the field of cyberspace, and it has stated that Article 5 can be applicable in case of a cyberattack against one of the Allies. Hence, in theory at least, it would make no difference if a country attacks one of NATO's Allies with 10 ballistic missiles, 1000 tanks or a cyberattack with an equivalent impact. Any of these actions could trigger the political decision to invoke Article 5. This decision is of major importance, since it has a significant impact on the strategic, and thus political, level of thinking, including on deterrence, operational planning and conduct. Such a decision might be taken, if an event – similar to the episode from Estonia (2007) – unfolds differently from the point of view of the deterrence calculations. Here applies one of the most important aspects of Article 5, which refers to NATO's capacity to deter the enemies from attacking, given the consequences, namely the response of the entire organisation (the musketeers' principle). In the case of the cyberspace, this aspect is more complex because deterrence here involves more than the classical fear of punishment (Caruson, MacManus and McPhee, 2012). As Nye Jr. (2017) highlights, we can speak about **four means of deterrence** when referring to cyber security: threat of punishment, denial by defence and resilience, entanglement, and normative taboos. Coming back to Article 5 and the consequences of applying it to the cyberspace, it is very important to emphasise that it will not be automatically triggered in the event of an attack. Firstly, the attacked country must demand its activation. To do that, the attack must cause such severe damage to its national security that the victim state cannot cope with it on its own. Consequently, it needs the help of the others. Secondly, as NATO Deputy Assistant Secretary General for Emerging Security Challenges, Jamie Shea, stated, NATO officials did not mention exactly which circumstances might trigger the Alliance's collective response, or which is the threshold that needs to be met. Also, they did not mention either which should be NATO's response (Ranger, 2014). These aspects are to be discussed by the Allies on a case-by-case basis. NATO only established that a cyberattack causing a certain level of damage could be treated as an armed attack, if it is conducted with a malicious intent in mind (Ranger, 2014). Hence, even if – in the aftermath of a cyberattack of great magnitude – the attacked country demands the activation of Article 5, all the Allies must decide whether they activate the musketeers' principle or not.

From a legal point of view, the activation is even more difficult to achieve. According to the Tallinn Manual 2.0, Rule 80, if cyber operations are executed in the context of an armed conflict, they are a subject of law (Schmitt, 2017, pg. 375). Therefore, if a state is cyber-attacked and the cyberattack reaches the threshold of an armed attack, then that state can invoke its right to self-defence (Schmitt, 2017, pg. 375). Thus, legally speaking, cyberwar is a matter of international law. Yet, as the above declaration stipulated, a cyberattack must be treated as an armed attack, and for that it must reach the threshold of such an act. In line with international law, the armed conflict was defined by the 1949 Geneva Convention, but *"has never been authoritatively defined as a matter of treaty law"* (Schmitt, 2017, pg. 375). Moreover, according to Rule 71, a cyberattack can be defined as an armed attack, depending on the effects of that specific action and its scale (Schmitt, 2017, pg. 375). As such, the 2007 Estonia attacks did not meet the damage threshold required for considering them at the scale of an armed attack. Also, Stuxnet poses a problem when discussed from the legal point of view, because although it caused physical damage, it is debatable if the damage level was high enough. Meanwhile, the situation becomes increasingly complex when we analyse it from the actors' point of view, since the international law does not encompass the activities conducted by individuals or other types of actions not related to armed conflict (Schmitt, 2017, pg. 377). So, there must be clear evidence that the company X, the group Z, or the individual A is acting on behalf of a state. Last but not least, there is the matter of attribution: NATO cannot respond to a cyberattack until the decision-makers are sure who is responsible for it, and this may take days, weeks, even months, and thus enough time for the attack to pass/end.

Next, our analysis will focus on NATO's actions and development when it comes to cyberspace, and how its member states adapted to this new security reality. This analysis is necessary in order to see how one of the most important alliances in the international system has adapted and acts in the field of cyberspace nowadays.

2.2. NATO

Despite the end of the Cold War, NATO's role remains indispensable. The Alliance pursued its role as a provider of collective defence in a very unstable globalised world. But, in order to ensure a proper and sustainable security environment, the organisation must be resilient, and quickly adapt to the new challenges of the 21st century. Thereby, we consider that in this part of our paper it is necessary to point out how NATO's approach and policy on cyber-defence evolved, and the main challenges faced by the member states during the last decades.

Here is a brief presentation of the historical steps taken:

- The Prague Summit in November 2002. It marked NATO's first attempt to tackle the cyber issue. For the first time, in a NATO strategic document, the Allies set the objective of strengthening their capabilities in order to defend against cyberattacks (NATO, 2002).
- The Riga Summit in November 2006. The military alliance planned to develop a NATO Network Enabled Capability with the purpose of improving protection against cyberattacks (NATO, 2006).
- In 2008, the "Cooperative Cyber Defence Centre of Excellence" from Estonia (CCDCOE) was accredited by the Allied Command Transformation, and endorsed by the NATO Council.
- The 2010 Lisbon Summit. NATO's Council pushed for developing a NATO cyber defence policy, and for an action plan to implement it (NATO, 2020).
- In 2011, NATO developed its first Policy on Cyber Defence whose main objective is to provide mutual and coordinated assistance, if one of its member states falls victim to a cyberattack (NATO, 2011).
- In 2012, the field of cyber defence was integrated into NATO's Defence Planning Process, and the NATO Communications and Information Agency (NCIA) was established (NATO, 2020). NCIA became the frontline against cyberattacks. It works closely with governments and private entities (NCIA, n.d.).
- In September 2014, at the Wales Summit, NATO took the strategic step of linking cyber defence to the "core business" of the Alliance, namely collective defence. The member states approved a new cyber defence policy, which recognised, for the first time, that cyberattacks might reach a threshold that can trigger a collective response under Article 5 of the Washington Treaty. At this Summit, NATO members decided to create

Cyber Rapid Reaction Teams to help mitigate the harmful cyberattacks, and to boost cooperation with the private sector on the management of cybersecurity threats, by launching a dedicated NATO Industry Cyber Partnership – NICP (NATO, 2020).

- In 2016, during the Warsaw Summit, NATO took an important decision, in terms of operationalizing cyber defence, by declaring cyber as a domain of military operations, along with land, sea, air (and later, in 2019, space). This decision had important implications for military planning and doctrine. It also entailed the potential planning and use of cyber offensive operations for defensive purposes, and with the observance of international law.
- In 2019, NATO's defence ministers approved a guide that set up a number of tools destined for strengthening the ability of member states to respond to cyberattacks (NATO, 2020).
- In 2023, at the Vilnius Summit and in the context of the Ukrainian war, member states proposed a new concept to enhance the cyber-defence contribution to NATO's deterrence and defence posture. In response to major malicious cyber activities, they established NATO's new Virtual Cyber Incident Support Capability (VCISC) to assist national mitigation efforts. This gives the Allies one more resource to help them and to improve the protection of Allies' capabilities against such threats (NATO 2023).

Following this timeline of the cyber evolution in NATO's strategic documents, we can see that the Alliance is adapting to the new challenges of the 21st century, since it has at its disposal forces that are both compatible and quick in their response (Efthymiopoulos, 2014, pg. 307). The most important measures for achieving interoperability and well-equipped forces (from a technological view) were the designing of a Cyber Defence Policy in 2011, and the inclusion of cyberspace among the operational domains in 2016. Yet, the need for a common cyber-defence approach (and, later, the need for strategy and policy) arose with the 2007 major cyberattack on Estonia's critical infrastructure (Stahl, 2011, pg. 250). It was a threat of such a scale that the Allies felt compelled to give a coordinated response both operationally and strategically. In the absence of clear evidences, one might say it was the first coordinated cyberattack on a sovereign state, conducted by the Russians. It affected the essential electronic infrastructure (such as servers) of banks, newspapers, or retail companies (Davis, 2007). In order to tackle this problem, Matthew Sklerov (2009, pg. 31) argues, it will be necessary to establish procedures and cooperate at international level. This has been achieved through the yearly "Cyber Coalition" (launched in 2013) exercise series, one of the biggest multinational cyber defence exercises in the world, which aims to improve the capacity of NATO Allies and partners to protect their networks and collaborate in cyberspace (Giordano, 2023). However, for a better coordination, the Allies need to know first the enemies they are facing. Apart from that, they need to tailor their response to those enemies, an issue that we shall elaborate on in the next chapter of this research.

Returning to the international level, the overall developments in this field have shown us that cyberspace has become an integral part of NATO's operative environment, as a response to the current conflicts and crises (Limnéll and Salonius-Pasternak, 2016, pg. 1). Hence, the framework was created, but it remains to be seen how effective it will be, given its limitations imposed by legal constraints, and the scope assigned to it by the existing specialised literature. In the following section, we shall focus on the third layer of analysis: the Allies' modalities of adaptation to this new security architecture.

3. Analysis

As previously mentioned, we have carried out an analysis on each ally's cybersecurity strategy in order to identify three elements: the actors perceived as being active in the cyberspace, the existing threats, and the reasons for conducting cyber operations.

All three are equally important for the present research, since one cannot even claim that he is trying to ensure his security without knowing his opponents (namely, the types of actors and the threats they pose). Additionally, to properly deal with these enemies / competitors, the decision-makers need to understand them, and thus to understand thoroughly the motives behind their actions, so that they might foresee their future actions, and develop efficient security instruments. Moreover, this comparison is necessary for assessing the degree of common views within the Alliance, since all NATO member states must have a similar view on the security constellation to ensure deterrence and, eventually, trigger Article 5. Therefore, we must discuss about a harmonisation of perceptions and future actions, which should lead to a harmonisation in setting the threshold. As shown below, nowadays we can rather speak about a heterogeneity, and not a homogeneity of views.

3.1. Actors

The table below highlights the nature of the actors in cyberspace divided into two large categories: state and non-state actors. Additionally, the latter category is split into three subcategories: criminal organisations, terrorist groups, and individuals. The distinction is very important because it indicates how each ally defines these actors, a fact likely to influence the national cybersecurity. This represents the starting point for a potential development of a common understanding of the cyber landscape.

Table 1. Actors in the cyberspace

State	State actors	Non-state actors		
		Criminal organisations	Terrorist groups	Individuals
Albania	x	✓	x	✓
Belgium	✓	✓	✓	x
Bulgaria	✓	✓	✓	✓
Canada	✓	✓	x	✓
Croatia	x	✓	✓	✓
Czech Republic	✓	✓	✓	✓

Denmark	✓	✓	x	✓
Estonia	✓	x	x	x
France	✓	✓	✓	✓
Germany	✓	✓	✓	✓
Greece	✓	✓	x	✓
Hungary	✓	x	x	x
Iceland	✓	✓	x	✓
Italy	✓	✓	✓	✓
Latvia	x	✓	x	✓
Lithuania	✓	x	x	x
Luxembourg	✓	✓	x	x
Montenegro	✓	✓	✓	✓
Netherlands	✓	✓	x	✓
North Macedonia	x	✓	x	✓
Norway	✓	✓	x	✓
Poland	✓	✓	✓	✓
Portugal	✓	✓	✓	✓
Romania	✓	✓	✓	✓
Slovakia	✓	✓	x	x
Slovenia	✓	✓	✓	x
Spain	✓	✓	✓	✓
Türkiye	✓	✓	x	✓
United Kingdom	✓	✓	✓	✓
United States of America	✓	✓	✓	✓

Source: Authors' own research.

As one can notice, according to their national cybersecurity strategies, NATO member states have rather different views on the nature of actors in cyberspace. Less than a half (12 out of 30) see both state and non-state actors (criminal organisations, terrorist groups, and individuals) as active parties in the cyberspace. Although the cyberspace is not geographically biased, we could create regional clusters of states with similar views, as a proof that geopolitics still matters. Thus, we can note that the Southern Flank (Italy, Spain, Portugal), and the Eastern Flank (Poland, Romania, the Czech Republic, Bulgaria) of the Alliance share common views on the matter. In our opinion, this should not be construed as a coincidence. Taking into consideration their geographical proximity, it is natural they have the general tendency to perceive threats in a similar way. For example, Romania, Poland, and the Czech Republic have seen the Russian Federation as a threat, due to various reasons, not only historic ones. Although, as previously mentioned, the cyber threats are, by their nature, non-geographical, the states still tend to suspect their traditional competitors/enemies, and this tendency is on the rise now with the war in Ukraine. Besides, the main regional powers – UK, France, and Germany – share this comprehensive view. Even in their case, the choice is quite explicable. All of them are seen and act as great powers. Thus, to be credible at the international level, they should be able to cope with the entire spectrum of threats. The USA has the same approach, being the only NATO member that openly describes other states – i.e., the Russian Federation, Iran, North Korea, and China – as threats to its national security (USA, 2018). At the same time, the USA has a particular approach, since it pinpoints cyberspace as an area of geopolitical competition between known actors. This posture on cybersecurity is rather predictable, as the main competitors to its superpower in this domain are China and, to a certain extent, the Russian Federation. As regards the other two, i.e., Iran and North Korea, they have had an antagonistic relationship with the United States for years. Moreover, they are considered "rogue states" in the international security system. Hence, it is likely that the superpower will respond to their actions. We could argue that this strategy of naming the threats is based on *the principle of offensive defence*, which puts aside *the deterrence-based strategic thinking* in favour of a more war-oriented one. This line of action was proposed in 2010 by scholars like Harknett, Callaghan, and Kauffman (2010).

On the other hand, in 2016, the UK had a rather comprehensive view on cyberspace. Throughout its cybersecurity strategy, the following actors were identified: *"Cyber criminals – individuals, Russian-language organised criminal groups (OCGs) in Eastern Europe, emerging threats from South Asia and West Africa [….], states and state-sponsored threats [….], terrorist organisations [….], hacktivists [….], 'Script Kiddies' (less skilled individuals who use scripts or programmes developed by others to conduct cyberattacks) [….], individuals or smaller organisations [….], and insiders"* (UK, 2016). All these rather concrete actors are absent from the 2022 strategy, as the decision-makers adopted then a more general, nuanced approach with regard to the identity of the cyber players (UK, 2022). Meanwhile, the rest of NATO Allies have chosen to concentrate on specific groups of actors. For example, Belgium defines the state actors in cyberspace as being either superpowers, or less wealthy states, and/or proxies, which transform the cyberspace into a field of power projection competition (Belgium, 2021). Conversely, Croatia does not mention at all the state actors (Republic of Croatia, 2015).

Usually, smaller powers tend to rely on the power projection of the international organisations they are part of: NATO, the EU, OSCE, and the UN. Such is the case of Romania, Slovakia, Poland, the Czech Republic, Croatia, the Baltic States, etc. This bandwagoning towards greater powers for balancing a larger threat (too costly to deal with on one's own) can be seen as a rational behaviour. On the other hand, great powers, like France (2015) or Germany (2021), mention NATO or the EU as organisations that enable them to project their power, as security providers. In its turn, Türkiye mentions NATO only as a contextual player that has developed its cybersecurity policy (Türkiye, 2016). Being a cyber superpower, the USA makes no mention of the organisation in its 2018 strategy (USA, 2018). This heterogeneity facilitates a rather high volatility of cyberspace, which by its nature is very dynamic. It also proves that the Allies do not have a common view on the actors in the cyberspace, and this can hinder the decision-making process, since the activation of Article 5 depends on the unanimous decision of the member states. Additionally, the nature of the actors renders the decision-making process more complex, as indicated below:

- If an attack is carried out by a state, the international law will be applied.
- If an attack is conducted by non-state actors acting on behalf or sponsored by states, the international law will also be applied.
- If an attack is conducted by a non-state actor not directly connected with a state (organised crime), the national law will be applied in the state that has jurisdiction over the incident. Yet, this is one of the most complicated issues to solve in the cyber field.
- If the attacker is an individual, the national law will be applied, and this will give rise to another debate about the sovereignty principle, and which state can claim its rights over the incident.

Although the above provisions are rather clear, from an empirical perspective the answers are not, due to the borderless nature of cyberspace. Another problematic aspect is the interpretation of the international regulations not designed to handle a field like cyberspace. From this point of view, the Tallinn Manual is very useful and yet it has its limits, because the international law itself is limited, as we discover when we try to apply it to the cyber domain. For example, *the sovereignty* (Schmitt, 2017, pp. 11-29) and *jurisdiction* (Schmitt, 2017, pp. 51-78) *principles* are at play in the case of an attack conducted from the soil of state A by an individual (who is citizen of state B) against a national company of state D located in state C. Other quintessential and difficult issues to address in the cyberspace, before initiating countermeasures, are the identification of the attacker, and the discovery of a direct link between non-state actors and a certain state. To make things even more complicated, there is no internationally agreed-upon definition of the concept of "armed conflict", which is thus open to various interpretations by the states, and this enables the setting of different thresholds. One generally accepted idea is that an armed attack must generate significant physical damage (Schmitt, 2017, pg. 381). This usually applies to the conventional war. Yet, in case of a cyberattack, physical damage is very rare. This, of course, does not mean that the attack per se does not have important consequences for the national security. Illustrative examples in this sense are the 2007 Estonia cyberattacks, classified by the experts as not having reached the threshold of an armed attack (Schmitt, 2017, pg. 376). Hence, even if Estonia had demanded the activation of Article 5, the latter would not have been legally possible.

Taking into consideration all these aspects (*the issue of attribution, the different norms that should be applied according to the actor types, and the limits of the current international law*), the activation of Article 5 proves to be very difficult, but clearly not impossible. It is important to recall that its activation is a political decision taken in specific political and security circumstances. It has been activated, following the World Trade Centre plane attacks, despite the little clarity for attribution, and in the absence of any precedent with regard to that type of attack.

Next, we shall analyse the threats recognised by each NATO member state in order to see if the Allies have a different perspective on the security constellation. This aspect is very important, since they need to have a common view on the national security threats, so as to reach the required unanimity for the activation of Article 5.

3.2. Threats

Table 2. Threats in the cyberspace

State	Cyber-attacks*	Cyber-crime	Cyber espionage	Cyber terrorism	Cyber sabotage	Information/ Cyber warfare	Hacktivism
Albania	✓	✓	x	x	x	x	x
Belgium	✓	✓	x	✓	x	x	x
Bulgaria	✓	✓	✓	✓	x	x	x
Canada	✓	✓	✓	x	✓	x	x
Croatia	x	✓	x	✓	x	x	x
Czech Republic	✓	✓	✓	✓	x	x	✓
Denmark	✓	x	✓	x	x	x	x
Estonia	✓	x	x	x	x	✓	x
France	x	✓	✓	✓	x	x	x
Germany	✓	✓	✓	✓	✓	x	✓
Greece	✓	✓	x	x	x	x	x
Hungary	x	x	x	x	x	✓	x
Iceland	x	✓	✓	x	x	✓	x
Italy	✓	✓	x	✓	x	x	x
Latvia	✓	✓	x	x	x	x	x
Lithuania	x	x	x	x	x	✓	x
Luxembourg	✓	x	x	x	x	x	x
Montenegro	✓	✓	✓	✓	✓	✓	✓
Netherlands	✓	x	✓	x	✓	x	✓
North Macedonia	x	✓	✓	x	x	x	x
Norway	✓	✓	✓	x	✓	x	✓
Poland	x	✓	✓	✓	x	✓	x
Portugal	✓	✓	✓	✓	✓	✓	✓
Romania	✓	✓	✓	✓	x	✓	✓
Slovakia	✓	✓	✓	x	x	x	x
Slovenia	✓	✓	✓	✓	x	x	x
Spain	x	✓	✓	✓	x	✓	✓
Türkiye	x	✓	✓	x	x	x	✓
United Kingdom	✓	✓	✓	✓	x	✓	✓
United States of America	✓	✓	✓	x	x	✓	x

Source: Authors' own research.

** In this case, we searched for the concept of cyberattack as such within the national cybersecurity strategies.*

As one can see, even the perceptions of threats among NATO members are quite different. For example, Belgium – in its 2019 Strategy – divides the existing threats into kinetic/non-kinetic, and conventional/non-conventional, mentioning cyberattacks only generically (Belgium, 2019), whereas the 2021 Strategy defines threats rather differently and more specifically: cybercriminals, foreign military and intelligence services, terrorist groups, and hacktivists (Belgium, 2021). At the same time, Norway is among the very few states that recognise cyberbullying as a threat to their national security (Norway, 2019).

Although all of them acknowledge the diversity of actors and threats in cyberspace, only two Allies officially recognise all the selected categories (Montenegro, and Portugal). This aspect is essential because it shows a high level of heterogeneity within the Alliance. Therefore, it would be, in principle, extremely difficult for all NATO members to see a cyberattack as reaching the threshold of an armed attack.

As far as cyberwarfare is concerned, only 11 states recognise it directly as a threat: Estonia, Hungary, Italy, Lithuania, Montenegro, Netherlands, Norway, Portugal, Romania, United Kingdom, and USA. Meanwhile, Norway, for example, takes into account the possibility of a war being generated by a cyberattack that is considered an armed attack (depending on its conditions, legitimacy, purposes, and consequences), and it highlights its right to self-defence under the UN rules (Norway, 2019). This view is also shared by the Netherlands, which invokes its right according to Article 51 of the UN Charter, if an (imminent) cyberattack takes place. Here the accent is on the scale of the cyberattack, its magnitude being the essential element that makes it an (imminent) armed attack (Netherlands, 2018). Simultaneously, the decision-makers acknowledge the difficulty of applying this principle due to the attribution issues (Netherlands, 2018). In its turn, Montenegro discusses the difficulty of labelling it as an armed attack from a legal point of view (Montenegro, 2018). Hence, the views on this subject are quite different, generating different thresholds, thus distinct behaviours. Moreover, none of the aforementioned states clearly mentions which is the threshold that has to be reached for a cyberattack to be considered an armed attack. At the same time, few of them view the possibility of triggering Article 51 as a very bold statement, and a rather exceptional measure that could materialise through a very limited set of actions.

As regards the inclusion of NATO's approach to the cyberspace (cyber as the fifth operational domain) in the Allies' national security strategies, there are only seven states that mention the Alliance's designation of cyber as an operational domain: the Czech Republic, Estonia, Hungary, Iceland, Italy, the Netherlands, and Slovakia. We can note that the majority of the states from this list are Central European. Interestingly enough, in terms of cost-sharing arrangements for NATO's total budget for the period 2021-2024, all the aforementioned states (except Italy and the Netherlands, which contribute with 8.7881%, and 3.4532% respectively) have a sharing rate of only 1% or below (NATO, 2021). From this angle, we can consider rational their decision to emphasise NATO's outlook on cyberspace, because militarily speaking it is more cost-efficient to be under the umbrella of a big security provider than to free ride, especially if your own investment is rather low.

As nowadays everything turns digital, and states are following the same path, a potential cyberattack against a state can translate into a threat to the national sovereignty. After we showed the cyber actors and the main threats perceived by NATO member states, it is important to understand the reasons behind the cyberattacks. This is a necessary step in order to have a comprehensive view on this field.

3.3. Reasons

Table 3. Reasons behind cyber operations

State	Political gains	Financial/ Economic gains	Strategic advantage	Prove superiority	Military advantage	Cyber espionage
Albania	x	x	x	x	x	x
Belgium	✓	✓	✓	✓	✓	x
Bulgaria	✓	✓	✓	✓	x	x
Canada	x	✓	✓	x	x	x
Croatia	x	x	x	x	x	x
Czech Republic	✓	x	x	x	✓	✓
Denmark	x	✓	x	x	x	x
Estonia	✓	✓	✓	x	x	x
France	✓	✓	x	x	x	✓
Germany	✓	✓	✓	x	x	✓
Greece	x	x	x	x	x	x
Hungary	✓	x	x	x	x	x
Iceland	x	✓	✓	x	x	x
Italy	✓	✓	x	x	x	x
Latvia	x	✓	x	x	x	x
Lithuania	x	x	x	x	x	x
Luxembourg	x	✓	x	x	✓	x
Montenegro	x	✓	x	x	x	✓
Netherlands	x	x	x	✓	✓	x
North Macedonia	x	✓	x	x	x	x
Norway	x	✓	x	x	x	✓
Poland	✓	x	x	x	x	x
Portugal	✓	✓	x	x	x	x
Romania	✓	✓	✓	x	x	✓
Slovakia	x	x	x	x	x	x
Slovenia	✓	✓	✓	x	x	✓
Spain	✓	✓	✓	x	x	x
Türkiye	✓	✓	✓	x	x	x
United Kingdom	✓	✓	✓	✓	x	x
United States of America	✓	✓	x	x	x	x

Source: Authors' own research.

According to *Table 3*, political gains (16 states out of 30) and economic ones (21 states out of 30) have been identified by NATO member states as the main reasons for committing cyberattacks, while few states perceive strategic or military advantages, proving superiority or cyber espionage as being the cause. The cyberattacks driven by political and economic gains are strongly connected with states, and criminal organisations. Both of these reasons, emphasised by the national cybersecurity strategies, are clearly reflected in the strategy of the USA (2018). At the same time, the USA considers the Russian Federation, Iran, China, and North Korea as direct threats to its security and the security of the Allies. Thereby, the Trump administration specifically identified five states as potential enemies, by pointing out that the economic and political instability are their main targets (USA, 2018).

Moreover, there are three states, which do not mention – in their national strategies – any of the reasons from the above table as root causes of cyberattacks: Albania, Croatia, and Greece. If we compare *Table 2* with *Table 1*, Albania's behaviour is rather understandable, since it recognises only cyberattacks and cybercrimes as being the main threats in the cyberspace. The significant 2022 cyberattacks, which had a countrywide impact upon Albania's IT infrastructure, might however determine some changes in approach. To date, the same approach seems to apply in the case of Greece. Similarly, Croatia views only cyberattacks and cyber-terrorism conducted by non-state actors as being the main threats to its national cybersecurity.

Though some cyber attackers seek to prove their superiority (this can apply to both state and non-state actors, but is particularly important for understanding individual hackers), only two states view this reason as significant for their national security: Bulgaria and the Netherlands.

Besides the information provided in *Table 3*, we found some other country-specific reasons that could not be included there. For example, the Czech Republic brings cyber vandalism to the table (Czech Republic, 2015), Poland places emphasis on terrorist or religious reasons (Poland, 2019), Portugal focuses on ideology (Portugal, 2019), Norway on sabotage and hybrid operations, while Lithuania talks about malicious software, which – in combination with a disinformation campaign – could lead to societal chaos (Lithuania, 2018). These reasons are specific to each country based on the local history, and the previous experiences that shaped its national strategy.

All in all, if one can notice a certain homogeneity in the case of cyber actors, the homogeneity criterion is difficult to apply to the threats perceived or to the reasons behind them. This shows a lack of harmonisation within the Alliance, which will translate into different behaviours and reactions in case of a cyberattack reaching the threshold of a damaging attack. This represents a vulnerability of the Alliance that could affect the efficiency of deterrence.

3.4. A European view?

The European Union (EU) has its own mutual assistance clause, similar to Article 5 of NATO, namely Article 42.7 TEU that officially includes cyberattacks (European Union External Action, 2022). It must be mentioned that, in spite of this similarity, the EU does not have the military dimension that NATO has. Thus, *"Article 42(7) TEU is consistent with commitments under NATO, which is and will remain the foundation of collective defence for its members."* (European Union External Action, 2022).

Comparing the above tables, we cannot claim there is a unitary European view on cyberspace and wartime situations. Although the majority of the European Allies are also members of the EU (the most developed organisation in terms of supranational competences at the international level, whose Member States cooperate easier, going beyond the minimum common denominator when it comes to national security matters), we still remain within the intergovernmental framework. Yes, the majority of the EU members see state and non-state players as the main actors in the cyberspace. Yet, there are huge differences between their strategic views: e.g., several states, like Belgium, Estonia, Hungary, Lithuania, Luxembourg, Slovakia, etc. do not see individuals as factors able to influence their national cybersecurity (see *Table 1*). Additionally, there are even greater discrepancies with regard to the terrorist groups active in the cyberspace: e.g., Estonia, Denmark, Greece, Hungary, the Netherlands, and others do not consider these groups as being challenging in the cyberspace in terms of national security. As regards the criteria included in *Table 2*, there are very few countries that acknowledge the importance of information/cyber warfare (Germany, Hungary, Lithuania, Portugal, Romania, and Spain), cyber sabotage (Germany, the Netherlands, and Portugal), and/or hacktivism (Belgium, the Czech Republic, Germany, Netherlands, Portugal, Romania, and Spain). As far as the motives for cyberattacks are concerned, the heterogeneity continues to apply (*Table 3*). Therefore, only a few EU Member States view cyber espionage as a threat to their national security (the Czech Republic, France, Germany, Romania, and Slovenia). The same situation applies if the rationale behind the cyberattack implies the will of the attacker to obtain strategic advantage or prove superiority. Unfortunately, we do not see yet a unity regarding the criteria we have employed within the limits of the present research, although this is desirable within an integration-based organisation.

Conclusions

Can a cyberattack be considered an act of war? Can and will NATO trigger Article 5 in the case of a cyberattack? These are the key questions we have tackled throughout the current article, by analysing the complexity of the cybersecurity landscape, the development of NATO's cyber policy, and the relevant aspects reflected in the Cyber Security Strategies of NATO members. The most important challenges we have faced, in responding to these key research questions, were posed by the novelty of the cyber domain; the need to accumulate and further analyse the experience of cyber-conflicts; the lack of legal clarity with respect to the armed-conflict threshold the cyberattack should reach; the rare instances in which a cyberattack caused significant physical damage; the lack of rapid attribution tools; the multitude of cyber actors; and the insufficient harmonisation of the Cyber Security/Defence Strategies among NATO members. But, if we were to give a clear answer, we could say that, yes, a cyberattack can be considered, in specific circumstances, an act of war, namely when its size and impact may generate a political decision to characterise it as an armed attack.

As regards the second question, in this paper we have analysed the cyber security strategy of each NATO member state, and we have shown how the Allies perceive this new type of security challenge. In the literature review, following Stone's and Joseph S. Nye Jr.'s points of view, we have considered the cyberwar as a type of bloodless war taking place in the virtual layers of cyberspace. However, the cyberwar is able to create physical destruction (Stuxnet), and generate billions of dollars in damage (SolarWinds). Moreover, such a war would still fall under Clausewitz's assumptions.

At the international level, an increasing number of states have become vulnerable to cyberattacks. Hence, NATO started to redefine its position on the cyberwar and the cyberspace. With time, the Alliance has changed its perception and understanding of cyberspace: it no longer sees it as a simple battlefield in a complex war, but as an operational domain. Therefore, cyberattacks and cyber-defence are now integrated in the NATO Doctrine and military planning as part of the multi-domain warfare approach. Due to multiple reasons and the variety of actors, the logic of the Cold War (where we were dealing with rational, and thus predictable, actors that had acquired the capability to destroy each other) cannot fully apply to this type of war. However, since the most potent cyber actors remain the nation states, the principles of *rationality* and *predictability* are still applicable to these actors. This very aspect has generated a high level of self-restraint at the level of state actors, which avoided a "Cyber Pearl Harbour" scenario until now. Yet, it is important to bear in mind that NATO does not provide clear guidelines or indications when a conventional attack is considered an act of war that would trigger the application of Article 5 (the collective defence clause). There is no automatic response or any precise attack threshold defined or indicated in any NATO policy or strategy that would trigger the collective defence clause. No such threshold is set for a conventional attack or cyberattack. The argument for this approach has to do with the concept of "strategic ambiguity". Allies deliberately maintain a level of ambiguity with regard to what would trigger a collective defence response under Article 5, no matter if it is a response to a conventional attack or a cyberattack. If all were clearly pre-defined, it would practically invite the attacker to act always below the pre-defined threshold, just to avoid a meaningful collective defence response. This also gives the Allies the necessary flexibility to choose the timing of their response (they are not obliged by a pre-defined threshold to respond automatically), the mix of actions, and the scale of the response. NATO's approach described above makes a lot of sense strategically, but to function properly, namely to efficiently and timely generate consensual political decisions, it needs a harmonisation of the national Cyber Security Strategies. Hence, finally, considering the different ways NATO Allies perceive the actors, the threats and the reasons of cyberattacks, we can conclude that a unanimous agreement on the activation of Article 5 is less likely to happen, due to the high level of heterogeneity of their views on the cyber landscape, and due to the very nature of the cyberwar.

References:

- Andress, J., and Winterfeld, S., 2014, *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*, Waltham: Elsevier.
- Angstrom, J., and Duyvesteyn, I., 2004. *Rethinking the Nature of War*, New York: Routledge.
- Banks, J., 2015, "The Heartbleed bug: Insecurity repackaged, rebranded and resold", *Crime Media Culture*, Vol. 11, Issue 3, pp. 1–21. Available at: https//doi.org/10.1177/1741659015592792.
- Belgian Defence, 2019, *Cyber Strategy for Defence*, Available at: https://ccdcoe.org/uploads/2018/10/Belgian-Defence-Cyber-Strategy-EN.pdf.

Accessed on: February 27, 2024.

- Belgium, 2021, *Cybersecurity Strategy Belgium 2.0 2021-2025*, Available at: https://ccdcoe.org/uploads/2018/10/Belgium_CCB_Strategy-2.0_2021_English.pdf. Accessed on: February 27, 2024.
- Bulgaria, 2018, *Cybersecurity Act*. Available at: https://dv.parliament.bg/DVWeb/showMaterialDV.jsp?idMat=131638. Accessed on: February 27, 2024.
- Canada, 2018, *National Cyber Security Strategy*, Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf. Accessed on: February 27, 2024.
- Caruson, K., MacManus, S-A., and McPhee, B-D., 2012, "Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success", *Journal of Homeland Security and Emergency Management*, Vol. 9, No. 2, Available at: https://doi.org/10.1515/jhsem-2012-0003.
- CCDCOE, 2008, "Centre is the first International Military Organization hosted by Estonia", Available at: https://ccdcoe.org/news/2008/centre-is-the-first-international-military-organization-hosted-by-estonia/. Accessed on: February 27, 2024.
- Clausewitz, Carl von, 2007, *On War*, New York: Oxford University Press,
- Czech Republic - National Security Authority, 2015, *National Cyber Security Strategy of the Czech Republic for the period from 2015 to 2020*. Available at: https://ccdcoe.org/uploads/2018/10/CZE_NCSS_en.pdf. Accessed on: February 27, 2024.
- Davis, J., 2007, "Hackers Take Down the Most Wired Country in Europe", Available at: https://www.wired.com/2007/08/ff-estonia/. Accessed on: February 27, 2024.
- Denmark - The Danish Government, 2018, *Danish Cyber and Information Security Strategy*, Available at: https://ccdcoe.org/uploads/2018/10/Denmark_danish_cyber_and_information_security_strategy_2018_English.pdf. Accessed on: February 27, 2024.
- Efthymiopoulos, M-P., 2014, "NATO's Cyber-Defence: A Methodology for Smart Defence" in *Cyber-Development, Cyber-Democracy and Cyber-Defense. Challenges, Opportunities and Implications for Theory, Policy and Practice*, edited by Elias G. Carayannis, David F.J. Campbell, and Marios Panagiotis Efthymiopoulos, New York: Springer.
- Ehrenfeld, J., 2017, "WannaCry, Cybersecurity and Health Information Technology: A Time to Act", *Journal of Medical Systems*, Vol. 41: Art. no. 104. DOI: 10.1007/s10916-017-0752-1. Available at: https://link.springer.com/article/10.1007/s10916-017-0752-1.
- Embroker, 2021, "2021 Must-Know Cyber Attack Statistics and Trends", Available at: https://www.embroker.com/blog/cyber-attack-statistics/. Accessed on: February 27, 2024.
- European Union External Action's website, *Article 42(7) TEU - The EU's mutual assistance clause*, 6 October 2022. Available at: https://www.eeas.europa.eu/eeas/article-427-teu-eus-mutual-assistance-clause_en. Accessed on: February 27, 2024.

- Farwell, J., and Rohozinski, R., 2011, "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy*, Vol. 53, Issue 1, pp. 23-40, DOI: 10.1080/00396338.2011.555586.
- Fidler, D., 2011, "Was Stuxnet an Act of War? Decoding a Cyberattack", *IEEE Security & Privacy*, Vol. 9, No. 4. DOI: 10.1109/MSP.2011.96.
- Foltz, A., 2012, "Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate", JFQ, Issue 67, 4th quarter 2012, Available at: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf.
- France, 2015, *French National Digital Security Strategy*, Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf. Accessed on: February 27, 2024.
- Germany, 2021, *Cyber Security Strategy for Germany 2021*, Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf.
- NATO, 2023, "NATO Exercises to Enhance Its Cyber Resilience," *NATO's ACT* (blog), November 20, 2023. Available at: https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/.
- Gray, C., 1999, "Clausewitz rules, OK? The future is the past – with GPS", *Review of International Studies*, Vol. 25, Issue 5, pp. 161–182. Available at: https://library.fes.de/libalt/journals/swetsfulltext/14965941.pdf. Accessed on: February 27, 2024.
- Greece, 2018, *National Cyber Security Strategy*, Available at: https://ccdcoe.org/uploads/2018/10/Greece_National-Cyber-Security-Strategy-ver.3.0_EN.pdf. Accessed on: February 27, 2024.
- Harknett, R-J., Callaghan, J-P., and Kauffman, R., 2010, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity", *Journal of Homeland Security and Emergency Management*, Vol 7, No. 1. Available at: https://doi.org/10.2202/1547-7355.1636.
- Hungary, 2013, *National Cyber Security Strategy of Hungary*, Accessed on: February 27, 2024. Available at: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf.
- IBM, 2020, *Cost of a Data Breach Report*, Available at: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf. Accessed on: February 27, 2024.
- Iceland - Minister of the Interior, 2014, *Icelandic National Cyber Security Strategy 2015-2026*. Available at: https://www.stjornarradid.is/media/innanrikisraduneyti-media/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf. Accessed on: February 27, 2024.
- Italy, 2013, *National Strategic Framework for Cyberspace Security*, Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/IT_NCSS.pdf. Accessed on: February 27, 2024.
- Jeske, D., McNeill, A-R., Coventry, L., and Briggs, P., 2017, "Security information sharing via Twitter: 'Heartbleed' as a case study", *International Journal of Web Based Communities*, Vol. 13, No. 2, pp. 172-192. DOI: 10.1504/Ijwbc.2017.10005189.
- Jibilian, I., and Canales, K., (2021), "The US is readying sanctions against

Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal", Accessed on: February 27, 2024. Available at: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

- Kaspersky, 2021, "What is WannaCry ransomware?", Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry. Accessed on: February 27, 2024.
- Lambeth, B., 1997, "The Technology Revolution in Air Warfare", *Survival: Global Politics and Strategy*, Vol. 39, No. 1. Available at: http://dx.doi.org/10.1080/00396339708442897.
- Larsdotter, K., 2005, "New wars, old warfare? Comparing US tactics in Vietnam and Afghanistan" in *Rethinking the Nature of War*, edited by Isabelle Duyvesteyn and Jan Angstrom, New York: Frank Cass.
- Latvia, 2019, *Cybersecurity Strategy of Latvia 2019–2022*, Available at: https://www.mod.gov.lv/sites/mod/files/document/Cybersecurity%20Strategy%20of%20Latvia%202019_2022.pdf. Accessed on: February 27, 2024.
- Lester, T., 2016, "Cyber security: A growing threat to the energy sector - an Australian perspective", Sydney, Australia. Available at: https://www.hoganlovells.com/en/knowledge/topic-centers/cybersecurity-solutions/~/media/c14b2cc829b04a6e841237f66882b2df.ashx. Accessed on: February 27, 2024.
- Limnéll, J., and Salonius-Pasternak, Charly, 2016, "Challenge for NATO – Cyber Article 5", *Center for Asymmetric Threat Studies (CATS)*. Available at: https://www.diva-portal.org/smash/get/diva2:1119569/FULLTEXT01.pdf. Accessed on: February 27, 2024.
- Lithuania, 2018, *National Cyber Security Strategy*, Available at: https://ccdcoe.org/uploads/2018/10/Lithuania_Cyber-Security-Strategy-2018_English.pdf. Accessed on: February 27, 2024.
- Luxembourg, 2021, *Luxembourg Cyber Defence Strategy*, Available at: https://ccdcoe.org/uploads/2018/10/Luxembourg_Cyber-Defence-Strategy_2021_English.pdf. Accessed on: February 27, 2024.
- Mattei, T., 2017, "Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack", *World Neurosurgery*. DOI: 10.1016/j.wneu.2017.06.104.
- McGraw, G., 2013, "Cyber War is Inevitable (Unless We Build Security In)", *Journal of Strategic Studies*, Vol. 36, Issue 1, pp. 109-119. DOI: 10.1080/01402390.2012.742013.
- Montenegro, 2018, *Cyber Security Strategy of Montenegro 2018-2021*. Available at: https://www.gov.me/dokumenta/fa4f3ed4-d059-4958-8847-d6111360a477. Accessed on: February 27, 2024.
- Morse, A., 2017, "Investigation: WannaCry cyber attack and the NHS", National Audit Office. Available at: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. Accessed on: February 27, 2024.

- NATO, 2002, "Prague Summit Declaration". Available at: https://www.nato.int/cps/en/natohq/official_texts_19552.htm. Accessed on: February 27, 2024.
- NATO, 2006, "Riga Summit Declaration". Available at: https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en. Accessed on: February 27, 2024.
- NATO, 2011, "Defending the networks. The NATO Policy on Cyber Defence". Available at: https://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf. Accessed on: February 27, 2024.
- NATO, 2020, "Cyber defence". Available at: https://www.nato.int/cps/en/natolive/topics_78170.htm. Accessed on: February 27, 2024.
- NATO, 2021, "Funding NATO". Available at: https://www.nato.int/cps/en/natohq/topics_67655.htm. Accessed on: February 27, 2024.
- NATO, 2023, "Vilnius Summit Communiqué Issued by NATO Heads of State and Government". Available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm.
- NCIA, 2021, "What we do". Available at: https://www.ncia.nato.int/what-we-do.html. Accessed on: February 27, 2024.
- Netherlands, 2018, *Defensie Cyber Strategie 2018 - Investeren in digitale slagkracht Nederland*. Available at: https://www.defensie.nl/downloads/publicaties/2018/11/12/defensie-cyber-strategie-2018. Accessed on: February 27, 2024.
- North Macedonia, 2018, *National Cyber Security Strategy 2018-2022*. Available at: https://ccdcoe.org/uploads/2021/02/North-Macedonia_National-Cyber-Security-Strategy-2018-2022_2018_English.pdf. Accessed on: February 27, 2024.
- Norway, 2019, *National Cyber Security Strategy for Norway*. Available at: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf. Accessed on: February 27, 2024.
- Nye Jr., S-J., 2011, "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, Vol. 5, No. 4, pp. 18-38.
- Nye Jr., S-J., 2017, "Deterrence and Dissuasion in Cyberspace", *International Security*, Vol. 41, No. 3, pp. 44–71.
- Poland, 2019, *Cybersecurity Strategy of the Republic of Poland for 2019-2024*. Available at: https://ccdcoe.org/uploads/2018/10/Poland_Cybersecurity-Strategy-of-Republic-of-Poland-for-2019-2024_original-3.pdf. Accessed on: February 27, 2024.
- Portugal, 2019, *National Strategy for Cyberspace Security (NSCS) 2019-2023*. Available at: https://ccdcoe.org/uploads/2018/10/Portugal_National-Strategy-for-Cyberspace-Security-2019-2023_English.pdf. Accessed on: February 27, 2024.
- Purplesec, 2021, "2021 Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends". Available at: https://purplesec.us/resources/cyber-security-statistics/. Accessed on: February 27, 2024.
- Ranger, S., 2014, "NATO Updates Policy: Offers Members Article 5

Protection Against Cyber Attacks". Available at: https://www.atlanticcouncil.org/blogs/natosource/nato-updates-policy-offers-members-article-5-protection-against-cyber-attacks/. Accessed on: February 27, 2024.

- Republic of Albania, 2018, *Cybersecurity Strategy 2018-2020*. Available at: https://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf. Accessed on: February 27, 2024.
- Republic of Croatia, 2015, *The National Cyber Security Strategy of the Republic of Croatia*. Available at: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf. Accessed on: February 27, 2024.
- Republic of Estonia, 2018, *Cybersecurity Strategy 2019-2022*. Available at: https://www.mkm.ee/media/703/download. Accessed on: February 27, 2024.
- Rid, T., 2012, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, Vol. 35, No. 1, pp. 5-32. Available at: http://www.creativante.com.br/download/Cyber%20War.pdf
- Romania, 2021, "Strategia de securitate cibernetică a României, pentru perioada 2022-2027, şi Planul de Acţiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027" [*Romania's Cybersecurity Strategy for 2022-2027, and the Action Plan for implementing Romania's Cybersecurity Strategy for 2022-2027*]. Available at: https://securitypatch.ro/wp-content/uploads/2022/01/Monitorul-Oficial-Partea-I-nr.-2Bis.pdf. Accessed on: February 27, 2024.
- Rusi, T., and Lehto, M., 2017 "Cyber threats mega trends in cyber space" in *ICCWS Proceedings of 12th International Conference on Cyber Warfare and Security*. Available at: http://books.google.com/books?id=uYiRDgAAQBAJ&pg=PA331&lpg=PA331&dq=rusi+lehto+Cyber+threats+mega+trends+in+cyber+space+pdf&source. Accessed on: February 27, 2024.
- Schmitt, M-N., 2017, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press. DOI:10.1017/9781316822524.
- Sklerov, M., 2009, "Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent", Available at: https://www.hsdl.org/?abstract&did=12115. Accessed on: February 27, 2024.
- Slovakia, 2021, *The National Cybersecurity Strategy 2021-2025*. Available at: https://ccdcoe.org/uploads/2018/10/Slovakia_National_Cybersecurity_Strategy-2021-2025_2021_English.pdf. Accessed on: February 27, 2024.
- Slovenia, 2016, *Cybersecurity Strategy: Establishing a System to Ensure a High Level of Cyber Security*. Available at: https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf. Accessed on: February 27, 2024.
- Smith, MLR, 2003, "Guerrillas in the mist: reassessing strategy and low intensity warfare", *Review of International Studies*, Vol. 29, No. 1, pp. 19-37. Available at: https://library.fes.de/libalt/journals/swetsfulltext/15245432.pdf.

- Soliman, T., De, Rajesh, Hungerford, J., Yoshihide, I., 2021, "Biden Administration Announces Expansion of Sanctions against Russia and Signals Potential Additional Restrictions Following SolarWinds Cyber-Attack". Available at: https://www.mayerbrown.com/en/perspectives-events/publications/2021/04/biden-administration-announces-expansion-of-sanctions-against-russia-and-signals-potential-additional-restrictions-following-solarwinds-cyber-attack. Accessed on: February 27, 2024.
- Spain, 2019, *National Cybersecurity Strategy*. Available at: https://www.ccn-cert.cni.es/en/about-us/spanish-cybersecurity-strategy-2013.html. Accessed on: February 27, 2024.
- Stahl, W., 2011, "The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity". Available at: https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1024&context=gjicl. Accessed on: February 27, 2024.
- Stone, J., 2012, "Cyber War Will Take Place!", *Journal of Strategic Studies*, Vol. 36, No. 1, pp. 101-108. DOI: 10.1080/01402390.2012.730485. Available at: https://flavioufabc.files.wordpress.com/2017/02/stone-cyberwar-will-take-place.pdf
- Turkey, 2016, *2016-2019 National Cyber Security Strategy*. Available at: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf. Accessed on: February 27, 2024.
- UK, 2016, *National Cyber Security Strategy 2016-2021*. Available at: https://assets.publishing.service.gov.uk/media/5a81914de5274a2e8ab54ae9/national_cyber_security_strategy_2016.pdf. Accessed on: February 10, 2024.
- UK, 2022, *Government Cyber Security Strategy. Building a cyber resilient public sector 2022-2030*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf. Accessed on: February 27, 2024.
- UN, *Charter of the United Nations*, n.d. Available at: https://legal.un.org/repertory/art51.shtml. Accessed on: February 27, 2024.
- USA, 2018, *National Cyber Strategy of the United States of America*. Available at: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Accessed on: February 27, 2024.
- Volz, D., 2017, "U.S. blames North Korea for 'WannaCry' cyber attack". Available at: https://www.reuters.com/article/us-usa-cyber-northkorea-idUSKBN1ED00Q. Accessed on: February 27, 2024.
- Watkins, B., 2014, "The Impact of Cyber Attacks on the Private Sector", MindPoint Group. Available at: http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf. Accessed on: February 27, 2024.
- Wilkinson, P., 2003, "The Changing Nature of War: New Wine in Old Bottles – A New Paradigm or Paradigm Shift?", *The Royal Swedish Academy of War Sciences: Proceedings and Journal*, Vol. 207, No. 1. Available at: https://www.kkrva.se/wp-content/uploads/Artiklar/031/kkrvaht_1_2003_2.pdf.