PRIVATE-PUBLIC PARTNERSHIPS IN CYBER SPACE AS DETERRENCE TOOLS. THE TRANS-ATLANTIC VIEW

Ana Maria COSTEA, PhD
National University of Political Science and Public Administration
Bucharest/Romania

Abstract
Nowadays technological development has brought new threats and risks that states need to face in cyberspace. Given the multitude of actors, reasons, strategies, various types of attacks, the classical way of viewing the state as the sole security provider no longer functions. In this framework, private companies gain more and more competencies and responsibilities, especially in the areas of critical infrastructure. The present article explores the role of public-private partnerships in the national cybersecurity strategies of each NATO member state as tools of deterrence. The paper starts by analysing the concepts of deterrence and resilience. Secondly, it emphasizes the view of NATO regarding the topic, this aspect being followed by each of the 31 NATO member states' most recent national cybersecurity strategies, highlighting the objectives, measures, and examples of PPPs that each state has in order to highlight the status-quo at empirical level.

Keywords
Cybersecurity; deterrence; national cybersecurity strategy; PPPs; NATO allies; resilience.

1.INTRODUCTION

Cybersecurity is nowadays among the most discussed topics at both empirical and theoretical levels, since it touches numerous levels of national and international security, involving a multitude of actors that have key roles in the decision-making process from the state authorities to private companies, non-state groups, scholars and the general public (Caruson, MacManus and McPhee 2012). This has generated a huge debate regarding the necessary tools to deal with the threats and vulnerabilities from this sector against national security, having scholars like Koch & Golling (2018) and Valeriano & Jensen (2019) discussing about the applicability of the traditional concepts and their tools in this new security environment.

In terms of victims, although the most known cyberattacks - Stuxnet (Fidler 2011), or the 2007 Estonian attacks (Ottis 2018), BlackEnergy (Aljohan 2022), to a certain extent Wannacry (the part of the attack that affected the hospitals from the UK (Morse 2017), the Russian Central Bank, Deutsche Bahn (Mattei 2017)-, were designed to specifically damage the state's national security, the majority of the cyberattacks had a private company as a victim - Sony (Bonne 2012), Solar Winds (Jibilian, Canales 2021), Heartbleed (Banks 2015), Wannacry since it affected also private entities like Fedex, Telefónica (Mattei 2017). In terms of financial losses, "Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next three years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015." (Morgan 2023) Other important elements that have to be added to the picture are represented by the very nature of the attackers, since the cyberspace is a field where the costs for conducting an attack are relatively low and the accountability for such actions can be rather limited due to, still, underdeveloped legal framework and due to technical issues regarding attribution. In this very dynamic security landscape, states have started to develop their national cybersecurity strategies, but they are not the only responsible actors in terms of providing security. It is very important to mention that in the majority of cases, the critical infrastructure is owned or operated by private companies, thus it is not a desideratum, but rather a necessity for the state to develop private-public partnerships (PPPs). At the

same time, nowadays states still tend to function from the Weberian point of view (Weber 1918), thus they are very reluctant to transfer part of their security competencies to private entities. On the other hand, it is also a matter of taking over security responsibilities by the private actors and going to security procedures like security clearances, state established standards, etc., aspects that are not always welcomed by some companies. Additionally, by accepting the state to transfer some of its security competences, a private company is also accepting the transfer of security responsibilities (Carr 2016, 44). And this is largely problematic for a state since providing security for its citizens is part of the very leitmotivs of its raison d'être (Cavelty, Suter 2009, 181). On the other hand, as mentioned above, important parts of the critical infrastructure are held or operated by private companies (electricity, water, transport, etc.), therefore without PPPs, it is questionable if states can provide a credible level of security (Carr 2016, 44). At the same time, private entities are very reluctant to give their information to states in case of a cyberattack for economic purposes since they can be seen as breaking the trust of their customers or since revealing their security vulnerabilities to the public can affect their national and international status. Hence, PPPs, although a necessity, are positioned in a rather ambiguous situation.

In order to break this ambiguity, the present paper aims to analyse how states view the PPPs in the cyber field from a security point of view. In order to do that, we will compare the national cybersecurity strategies of all NATO member states, since NATO is among the most structured and developed security organizations. Another reason why we have chosen NATO is represented by the effects of the Ukrainian war on the Trans-Atlantic security and the cyber activities that the Russian Federation has employed over the years against NATO allies. Also, we have to mention the strategic competition with China and the Chinese behaviour in the cyberspace (NATO Cyber Defence 2023). This analysis is of high importance since all NATO member states view national security in a similar manner and all of them have adopted their own national cybersecurity strategies. Last, but not least, NATO is the sole alliance that would officially go to war in case of a cyberattack since in 2016 the cyberspace became an operational domain; thus, it would fall under the Article 5 framework

(NATO Cyber Defence 2023). If we enlarge the spectrum of organisations (economic, political ones), we could also add the EU. It has a similar provision, Article 42.7 of TEU, when the EU decision-makers take into consideration its activation in case of a cyberattack (European Union External Action 2022). At the same time, the EU is not a military organisation, nor does it intend to be on short and medium term, hence "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).

From a methodological point of view, the first part of the paper will encompass the existing literature review regarding the concepts of resilience and deterrence. We will use the concept of deterrence from Nye Jr's (2017) point of view since we cannot reasonably have a high level of deterrence by denial without reaching a suitable level of resilience. Additionally, a state cannot be resilient against an attack on its critical infrastructure (part of its national security sectors (Buzan 1991) without having mutually beneficial cooperation with the private sector, since many of the infrastructure elements are held or operated by it. Secondly, we will analyse NATO's development and point of view regarding these aspects, since deterrence was and still is a core element of its strategy. The paper will not argue the capacity of NATO to deter through punishment, thus its nuclear power projection, but it will focus on the development of PPPs in the cyberspace. Last, but not least, all NATO member states' cybersecurity strategies will be analysed and compared. The first element that we will look at is to see if they have the desideratum of cooperation between the public and the private domains as a strategic objective in their programmatic documents. We will also analyse how they view this relationship, as a need to cooperate, thus allowing the possibility of a top-down approach, or as a partnership, thus employing equal grounds. Secondly, we will identify the measures (if they exist) that the states propose in order to develop or deepen the PPPs. Last, but not least, we will go beyond the strategic documents when the situation imposes it to see possible examples of PPPs and their areas of cooperation. Since some allies have adopted over the years several national cybersecurity strategies, the present paper will take into consideration the most recent one for each state. Regarding the timeframe, the analysis will encompass

the period of 2007-2023, when the Estonian attacks took place (Ottis 2018) and 2023 since this was the year of adoption of the USA (*National Cybersecurity Strategy* 2023) and Latvia's (*The Cybersecurity Strategy of Latvia 2023-2026* 2023) latest programmatic documents. In terms of limitations, for the national cybersecurity strategies that are not available in English or Romanian, unofficial translations have been conducted.

2. LITERATURE REVIEW

Taking into consideration the multitude of traditional and non-traditional threats, one concept that stays at the core of nowadays strategic thinking is resilience. Walker and Salt (2006) describe it as being a system's capacity to evolve in a constant manner and to adapt to the occurring disturbances and maintain its core functions and structure simultaneously. In NATO's terms, it represents "the individual and collective capacity to prepare for, resist, respond to and quickly recover from shocks and disruptions, and to ensure the continuity of the Alliance's activities" (*Resilience, civil preparedness and Article 3* 2023)[1]. Although the concept is not novel – taking into account that it appeared around the 2000s – its emergence at the national strategic level can be traced back to 2010 when several countries included it in their strategies or even adopted their own resilience strategies (e.g., Canada) (Svitkováa 2017, 24-26). One possible reason would be the constantly evolving nature of non-conventional threats that forced states to adapt due to the very fast technological development. At the same time, resilience implies the existence of other players – other than states - that can have a role in the security-providing process. Actually, it opens the debate regarding the function of a state as the sole security provider for its citizens, since we can have social, environmental, industrial,

[1] For more information regarding resilience and NATO please see: Ducaru, Sorin.2016. The cyber dimension of modern hybrid warfare and its relevance for NATO. *Europolity-Continuity and Change in European Governance*, *10*(1), 7-23. https://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf.

financial crises, and terrorism incidents that imply other actors' response, not only the state's (Fjäder 2014, 128). Another important aspect regarding resilience is that it implies the adaptability of an actor in a given situation, thus it assumes not if an attack is going to happen. Rather than that, it refers to when and how the attack will happen, and how the state is to respond, an aspect that reflects the constant threat evolution in the cyberspace.

Additionally, resilience is one of the main elements that make deterrence a credible asset, especially if we refer to the latter in Nye Jr.'s (2017) view. Deterrence does not refer solely to one's capacity to punish the attacker, thus making the enemy fear the costs of retaliation (threat of punishment). It can also refer to one's capacity to deny its attacker the satisfaction of the attack (by denial), by being able to defend, recover, and respond to the attack, thus resilience. Also, deterrence can encompass the situation in which the inter-dependence between the units is so high, that an attack would affect both of them (through entanglement). Last, but not least, Nye emphasizes a framework of functioning regulatory norms that would make one deterred from attacking for fear of losing its power projection status at the international level (through normative taboos) (Nye Jr 2017, 55-60). It is worth mentioning that the concept of deterrence is by itself problematic when applied in the cyberspace. First, it is the matter of attribution, in the sense that it is very difficult to find who was behind the attack due to the current technological development. Also, the nature of the attacker is highly problematic given the heterogeneous nature of the non-state actors (individual hackers, organized hacker groups, decentralized groups, organized crime groups, terrorists, etc.). Regarding the second type of deterrence (by denial), in order to be able to discourage the attacker from employing an offensive action against it, the state needs to know what threat it is defending against. In the cyber world, there is no ultimate weapon, as the nuclear bomb stands for the traditional framework. Here is where the partnership with the private companies is quintessential since non-public entities tend to invest more in their own protection, they own or have the right to operate certain parts of critical infrastructure of the state, and their reach goes beyond the national borders and they tend to be more flexible and make final decisions faster than the bureaucratic apparatus of the state (Lilli 2021, 182-183).

Last, but not least, in the words of Dunn Cavelty and Brunner, "technological development enhances two trends that diminish the importance of the state, both of which have implications for security: increasing internationalisation and increasing privatisation" (Cavelty, Brunner 2007, 8-9). Hence, the concept of deterrence in cyberspace generated a debate in the academic world. On one hand, its supporters claim its effectiveness[1], while, on the other hand, scholars perceive it as having limited applicability[2]. On top of that, the concept of cyberwar, especially in *Clausewitzian* terms, is also highly debated in strategic studies[3]. Given the topic at hand, we will concentrate on PPPs as resilience-related defence tools for national cybersecurity purposes, thus on deterrence by denial, because in cyberspace resilience is maybe the most efficient strategy that a country could adopt, given the multitude of threats and their very changing nature. In this framework, PPPs are crucial, since parts of the critical infrastructure are held or operated by private companies, thus, in case of a cyber-attack both the public and private security would be jeopardized. This creates the need for states to develop partnerships with the private actors. Having said that, the case study of NATO is even more important, since one of the fundamental elements that make the alliance efficient is represented by

[1] For more information see Kello, Lucas. 2017. *The virtual weapon and international order.* Yale University Press; Lindsay, Jon; Gartzke, Erik. 2019. Cross-domain deterrence: Strategy in an Era of complexity. Oxford University Press.

[2] For more information see Fischerkeller, Michael; Harknett, Richard. 2017. "Deterrence is not a credible strategy for cyberspace". Orbis, 61(3), 381- 393. https://doi.org/10.1016/j.orbis.2017.05.003; Lupovici, Amir. 2016. "The "attribution Problem" and the social construction of "violence": taking cyber deterrence literature a step forward". International Studies Perspectives, 17(3), 322–342. https://doi.org/10.1111/insp.12082.

[3] For more information please see: Stone, John. 2013. "Cyber War Will Take Place!". Journal of Strategic Studies. 36:1, 101-108. DOI: 10.1080/01402390.2012.730485.;Junio, Timothy. 2013. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate". Journal of Strategic Studies. 36:1, 125 -133, DOI: 10.1080/01402390.2012.739561.; McGraw, Gary. 2013. "Cyber War is Inevitable (Unless We Build Security In)". Journal of Strategic Studies. 36:1, 109-119, DOI: 10.1080/01402390.2012.742013. and Rid, Thomas. 2012. "Cyber War Will Not Take Place". Journal of Strategic Studies. 35:1, 5-32. http://www.creativante.com.br/download/Cyber%20War.pdf

deterrence, an element that stays at the core of Article 5. At the same time, it would be highly problematic for NATO to activate Article 5 over a cyberattack that took place against an ally's critical infrastructure that is owned/operated by a private company. Thus, deterrence through punishment in this case would have its practical and legal constraints. Having said that, deterrence by denial would, again, be the desirable approach. But, for this strategy to work, like any deterrence-based behaviour, it needs to be credible and in order to do that, states need to closely cooperate and coordinate with their private partners.

NATO decision-makers acknowledged the need to cooperate with the private sector[1] since 2014, when the NATO Industry Cyber Partnership was created (*NATO Industry Cyber Partnership*), thus even before cyberspace became an operational domain. In the following years, it reinforced the very nature of cyberspace as being of public-private character (*NATO Cyber defence* 2023) – an approach that was adopted in one way or another by the majority of NATO member states. The next section examines the different views in which each NATO ally positions itself in this framework in order to see if from a programmatic security-based perspective states are willing and can employ these partnerships for resilience, and ultimately, deterrence purposes.

3.NATO MEMBER STATE NATIONAL CYBERSECURITY STRATEGIES

Within the aforementioned security architecture, NATO quickly responded to the security dynamics, especially after 9/11 and the 2002 Prague Summit when it set the objective of protecting the alliance against cyberattacks. Here we have to also mention the 2007 Estonian cyberattacks that represented a turning point for what later would be a new operational domain within NATO (*Warsaw*

[1] For more information please see: Ducaru, Sorin. 2017. The security of critical energy infrastructure in the age of multiple attack vectors: NATO's multi-faceted approach. Europolity-Continuity and Change in European Governance, 11(1), 5-20. https://europolity.eu/wp-content/uploads/2017/06/Europolity_vol.11_no.1_-2017_art01_Ducaru.pdf.

Summit Communiqué 2016). The 2016 moment is of crucial value since cyber was included within the Article 5 scope of action, thus NATO would go to war if a cyber-attack against an ally reached the necessary threshold. It is highly debated if a war is possible in this case due to: the legal limitations of defining an armed attack, the attribution issue in the cyberspace, the multitude of state and non-state actors and their reasons, and rationality. But one cannot challenge the deterrence-related reasons and their strategic value that stood behind the political decision from the Warsaw Summit. Therefore, again, deterrence by denial seems to be the suitable approach. But in order for deterrence to work, it needs to be credible in the eyes of one's enemies. From this point of view, the article 5 provisions, the history of NATO, the partnerships among the allies and the assumed liberty to respond in whatever manner the NATO members find suitable (cyber or kinetic cyber-attacks), deterrence through punishment seems credible. But, when referring to deterrence by denial, especially when dealing with PPPs, a non-unitary view is highly problematic. From this point of view, beyond NATO's framework, each member state adopted its own national cybersecurity strategy that portrays its view of the necessary instruments that it has or needs in order to protect itself. As aforementioned, since states are not the only players, they needed to acknowledge the role that the private entities are holding as well. Additionally, the cyberspace by nature cannot be grounded to specific sectors, borders, types of players, types of attacks, etc. Although traditionally, the best defence is the offence (deterrence through punishment), in the cyberspace this strategy is rather problematic since there is no ultimate weapon that everybody fears like the nuclear one. Even if a state is constantly developing its offensive capabilities, the very fast speed of the technological development and the multitude of players makes this strategy unrealistic. Ultimately, in cyberspace, once the attack is released, the technical experts will have access to its details, thus it could be replicated or even developed in a more dangerous way. And if it is a zero-day vulnerability as it was in the case of Stuxnet, once released, the technical team will patch the system. Therefore, it is very difficult to develop an ultimate weapon in this field. In this context, deterrence by denial becomes one of the most feasible strategies. One way to

achieve this would be the development of a resilient system and PPPs are one way to do it especially when dealing with critical infrastructure.

As it can be seen below, all NATO allies have adopted as their strategic objective the partnership between the state and the private sector acknowledging this need. At the same time, it is worth mentioning that the level of development is very different from state to state. For example, in the case of Albania (*The National Cybersecurity Strategy and its Action Plan 2020-2025* 2020, 5), the strategy aims to identify the critical infrastructure sectors for which there is shared responsibility with the private sector. Additionally, from a defence point of view, the strategy aims to encourage and compel "all critical and important information infrastructure to develop strategic plans in case of cyberattacks and to take measures to withstand these attacks and to recover the damages or eliminate these attacks" (*The National Cybersecurity Strategy and its Action Plan 2020-2025* 2020, 11), revealing a resilient based strategy between the pubic and the private that is at the beginning stages of development. The same case applies to Hungary (*Government Decision 1838/2018 (XII.28.) on the Strategy for the security of network and information systems in Hungary* 2018, 2, 17) as well, since in its strategy, it proposes the development of shared responsibility between the public and the private through the establishment of cooperation between the actors. On the other hand, there are states like Belgium (*Cybersecurity Strategy Belgium 2.0 2021-2025* 2021, 30), which already developed cooperation and coordination-based platforms like Cyber Security Coalition, an institution that encompasses around 100 active members. This measure was necessary from a security point of view since for example "almost all of the internet's infrastructure and systems are in the hands of private owners" (*Cybersecurity Strategy Belgium 2.0 2021-2025* 2021, 22). Thus, in order to have a comprehensive and realistic view of the cybersecurity dynamics that are happening on Belgian soil, the strategy highlights the importance of the Centre of Cybersecurity Belgium, which has a coordinating role (*Cybersecurity Strategy Belgium 2.0 2021-2025* 2021, 33). Denmark also acknowledges the importance of private companies for its national security. However, it sees them as a vulnerability for the state' and the society's national security (*Danish Cyber and Information Security Strategy* 2018, 8). In order to tackle this weakness, the state proposes the

establishment of partnerships between them (*Danish Cyber and Information Security Strategy* 2018, 18-33). For Germany, according to its strategic documents, the cooperation between the public and the private is an obligation (*Cyber Security Strategy for Germany 2021* 2021, 9), highlighting an already established partnership and giving concrete examples of PPPs (alliances for cybersecurity: the UP KRITIS public-private and Cyberbündnis mit der Wirtschaft) and how they are beneficial for the German security (*Cyber Security Strategy for Germany 2021* 2021, 20, 53, 58). The same can be said about Italy which gives concrete examples of PPPs (*National Cybersecurity Strategy 2022 – 2026* 2022, 17). Additionally, ENISA also identifies clear PPPs examples like: Digital Innovation Hub (DIH), National Competence Centres, National Framework for Cybersecurity and Data Protection and National Technological Clusters[1]. Another positive example would be the Netherlands, which for years has been seen as a promoter of cooperation and shared responsibilities between private companies and public authorities. This vision is continued in its 2022 cybersecurity strategy (*Netherlands Cybersecurity Strategy 2022-2028* 2022, 15), where concrete examples of PPPs and their importance for national security are emphasized: The Dcypher platform and the Nationwide Network of Cybersecurity Partnerships (LDS) (*Netherlands Cybersecurity Strategy 2022-2028 2022*, 8-13). Other states like the Czech Republic see the cooperation between the public and the private in a more limited way, the strategy referring only to science and research in order to ensure the cyber defence of the state (*Cyber Defence Strategy of the Czech Republic 2018 –2022* 2018, 9). Therefore, although acknowledged by all, the PPPs are seen differently by each member state. Additionally, there are also very different levels of development in this area, emphasizing the existent heterogeneity within the alliance. Regarding resilience, for example Luxembourg is clearly aiming towards that direction: "Luxembourg Defence will contribute to enhancing national cyber competence in order to increase national cyberspace resilience across private and public sectors"

[1] For more information please see: ENISA's official website, *National Cyber Security Strategies - Interactive Map* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Italy

(*Luxembourg Cyber Defence Strategy* 2021, 12). The same can be said about Slovakia (*The National Cyber Security Strategy 2021-2025* 2021, 18), which clearly acknowledges the fact that the state needs a resilient private sector since it operates its critical infrastructure.

Secondly, the majority are very explicit regarding the measures that the state will take in order to reach the PPPs, with only a few exceptions like Bulgaria, Luxembourg, Norway and Slovenia. Apart from the examples that we have already mentioned, unfortunately, an objective without a concrete measure is counterproductive when referring to a resilience-based strategy. The number of states that already pinpoint existing functioning PPPs is lower (19 countries from the total of 31), emphasizing once again the very different levels of development within the alliance.

Last, but not least, the fact that the working strategies expand to this very large period of time contributes further on to the alliance's heterogeneity. From 2015, when France or Croatia adopted their strategies, to 2016 when Slovenia adopted its own, until 2023, we have witnessed several major attacks, as we have seen above. Thus, the cybersecurity landscape has suffered major changes. Also from the point of view of the technological development timeframe, this can be seen as tens of years. Further, another element that has to be highlighted is represented by the fact that each country has its own view over the strategy's implementation period, from 1 year, like the United Kingdom, to 15 years, like Iceland. Naturally, their objectives and measures will differ. Again, since the cybersecurity landscape if very fast changing, this can also be problematic. This element could be interpreted as the state's level of interest regarding its cybersecurity development or how much they are targeted by cyber-attacks. From this point of view, the USA and United Kingdom prove a very high political interest in the domain, the former changing its strategy once Biden came into power (thus each president coming with his own perspective over the issue) and UK adopting one yearly.

Returning to the concept of resilience through PPPs, which in turn can create a strategy based on deterrence by denial, it is rather problematic to claim that all NATO member states reach a credible level of development. There are still states that discuss either about identifying the public-private actors in the cyberspace

or propose initial cooperation steps, a fact that in nowadays entangled society comes unfortunately very late. Hence, without a robust cooperation framework and concrete and efficient PPPs, deterrence by denial remains a desideratum and the states rely on the traditional understanding of the famous article 5.

Table 1: NATO member states national cybersecurity strategies, PPPs views

		Latest National cybersecurity strategy	**Strategic objective**	**Measures**	**PPPs**
1	Albania	2020	✓	✓	
2	Belgium	2021	✓	✓	✓
3	Bulgaria	2016	✓		
4	Canada	2018	✓	✓	✓
5	The Czech Republic	2018	✓		✓
6	Croatia	2015	✓	✓	
7	Denmark	2018		✓	
8	Estonia	2019	✓	✓	✓
9	Finland	2019	✓	✓	✓
10	France	2015	✓	✓	✓
11	Germany	2021	✓	✓	✓
12	Greece	2020	✓	✓	
13	Hungary	2018	✓	✓	

		Latest National cybersecurity strategy	Strategic objective	Measures	PPPs
14	Iceland	2022		✓	
15	Italy	2022	✓	✓	✓
16	Latvia	2023	✓	✓	✓
17	Lithuania	2018	✓	✓	✓
18	Luxembourg	2021	✓		✓
19	Montenegro	2018	✓	✓	✓
20	Netherland	2022	✓	✓	✓
21	North Macedonia	2018	✓	✓	
22	Norway	2019	✓		
23	Poland	2019	✓	✓	✓
24	Portugal	2019	✓	✓	
25	Romania	2022	✓	✓	✓
26	Slovakia	2021	✓	✓	✓
27	Slovenia	2016	✓		
28	Spain	2019	✓	✓	✓
29	Turkey	2020	✓	✓	
30	UK	2022	✓	✓	✓

		Latest National cybersecurity strategy	Strategic objective	Measures	PPPs
31	USA	2023	✓	✓	✓

Source: Author's own elaboration based on the cybersecurity strategies of NATO member states[1]

[1] In order to do develop this research, we have extracted the objectives the concrete measures and the PPPs that are envisioned by each NATO ally in their national cybersecurity strategies. For more information regarding each strategy, please see: Albania. 2020. *Decision No. 1084, dated 24.12.2020 On Adopting The National Cybersecurity Strategy and its Action Plan 2020-2025.* https://www.unicef.org/albania/media/3526/file/Albanian_National_Cybersecurity_Strategy.pdf; Belgium. 2021. *Cybersecurity Strategy Belgium 2.0 2021-2025*. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf; Bulgaria. 2016. *Национална стратегия за киберсигурност „Киберустойчив а България 2020"* [National cyber security strategy. Cyber resilient Bulgaria 2020]. http://www.cyberbg.eu/doc/20161024_Cyber_strat_proekt.pdf; Canada. 2018. *National Cyber Security Strategy Canada's Vision for Security and Prosperity in the Digital Age*. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf; Czech Republic. 2018. *Cyber Defence Strategy of the Czech Republic 2018–2022*. https://www.vzcr.cz/uploads/69-Cyber-Defence-Strategy-2018.pdf; Croatia. 2015. *The National Cyber Security Strategy of The Republic of Croatia.* https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf; Denmark. 2018. *Danish Cyber and Information Security Strategy 2018-2021.* https://en.fm.dk/media/15468/danishcyberandinformationsecuritystrategy_weba.pdf; Estonia. *Cybersecurity Strategy Republic of Estonia 2019-2022*.https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia;
Finland. 2019. *Finland´s Cyber security Strategy 2019.* https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf;
France. 2015. *French National Digital Security Strategy*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf;
Germany. 2021. *Cyber Security Strategy for Germany 2021.* https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=9CB9A479E1496EA1F994129BB137F3D5.live892?__blob=pu

blicationFile&v=4; Greece. 2020. *National Cybersecurity Strategy 2020 – 2025*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece; Hungary. 2018. *Government Decision 1838/2018 (XII.28.) on the Strategy for the security of network and information systems in Hungary*. https://nki.gov.hu/wp-content/uploads/2020/11/Strategy-for-the-security-of-network-and-information-systems-in-Hungary.pdf; Iceland. 2022. *Icelandic National Cybersecurity Strategy 2022–2037*. https://www.stjornarradid.is/library/04-Raduneytin/Haskola---idnadar--og-nyskopunarraduneytid/Icelandic%20National%20Cybersecurity%20Strategy%202022-2037.pdf; Italy. 2022. *National Cybersecurity Strategy 2022-2026*. https://www.acn.gov.it/ACN_EN_Strategia.pdf; Latvia. 2023. *The Cybersecurity Strategy of Latvia 2023-2026*. https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf; Lithuania. 2018. *Government of the Republic of Lithuania Resolution on the Approval of the National Cyber Security Strategy*.https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/27107170d04511e8a82fc67610e51066?jfwid=dg8d31595; Luxembourg. 2021. *Luxembourg Cyber Defence Strategy*. https://defense.gouvernement.lu/dam-assets/la-defense/Luxembourg-Cyber-Defence-Strategy.pdf; Montenegro. 2017. *Cybersecurity strategy of Montenegro 2018-2021*.https://afyonluoglu.org/PublicWebFiles/strategies/Europe/Montenegro%202018-%202021%20National%20Cyber%20Security%20Strategy-EN.pdf; Netherlands. 2022. *Netherlands Cybersecurity Strategy 2022-2028. Ambitions and actions for a digitally secure society*. https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028; Republic of Macedonia. 2018. *Republic of Macedonia National Cyber Security Strategy 2018-2022*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NS%20Cyber%20Security%202018-2022_ENG.pdf; Norway. 2018. *National Cyber Security Strategy for Norway*. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf; Poland. 2019. *Cybersecurity Strategy of the Republic of Poland For 2019-2024*. https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/poland-cybersecurity-strategy-republic-poland-2019; Portugal. 2019. *National Strategy For Cyberspace Security 2019-2023.* Resolution of the Council of Ministers No. 92/2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/portuguese-ncss/@@download_version/ae00f93801664a57b22f9f5f96c1cd01/file_en; Romania. 2022. *Strategia de securitate cibernetică a României pentru perioada 2022-2027 [Romania's cybersecurity strategy for 2022-2027].* Decision no. 1.321/2021. https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128; Slovakia. 2021. *The National Cyber Security Strategy 2021-2025.* https://www.nbu.gov.sk/wp-

4.CONCLUSIONS

Given nowadays security architecture, the risks and threats that states need to respond to, PPPs are not only desirable, but they represent the necessary instrument for any state that wants to reach a suitable level of resilience, thus, security. Although the development levels of PPPs are very different across NATO member states, it is a quintessential element that all allies have adopted this cooperation-based relationship in their strategic documents. Although we cannot claim that deterrence by denial is actively and realistically working when referring strictly to PPPs in cyberspace, it is for sure the strategy that all NATO states are aiming for in the short, medium, and long term. Referring strictly to the status-quo, unfortunately the NATO member states are too diverse in their view over PPPs in the cyberspace, a fact that ultimately affects one of the most important elements of deterrence, credibility. Therefore, having states in the early stages of PPPs cooperation development, a functioning resilience-based strategy can be seen as unpractical, thus missing its own purpose. Until this situation changes, the alliance can still count on the classical strategy, deterrence through punishment, cyber being an operational domain and NATO having nuclear powers within its ranks.

---

content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf; Slovenia. 2016. *Cyber Security Strategy Establishing a System to Ensure a High Level of Cyber Security*. https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf; Spain. 2019. *National Cybersecurity Strategy*. https://www.dsn.gob.es/eu/file/2989/download?token=EuVy2lNr; Turkey. 2020. *National Cybersecurity Strategy 2020-2023*. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf; United Kingdom. 2022. *Government Cyber Security Strategy. Building a cyber resilient public sector 2022-2023*. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf; United States of America. 2023. *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

REFERENCES

- Albania. 2020. *Decision No. 1084, dated 24.12.2020 On Adopting The National C ybersecurity Strategy and its Action Plan 2020 - 2025.* https://www.unicef.org /albania/media/3526/file/Albanian_National_Cybersecurity_Strategy.pdf
- Aljohan, Tawfiq. 2022. *Cyberattacks on Energy Infrastructures: Modern War Weapons*. https://arxiv.org/ftp/arxiv/papers/2208/2208.14225.pdf.
- Banks, James. 2015. "The Heartbleed bug: Insecurity repackaged, rebranded and resold". *Crime Media Culture* 11, 3: 1-21. DOI: 10.1177/174165901559279 2.
- Belgium. 2021. *Cybersecurity Strategy Belgium 2.0 2021- 2025*. https://ccb.bel gium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf.
- Bonne, Lance. 2012. "Cyber Risk: How the 2011 Sony Data Breach and the Need for Cyber Risk Insur Cyber Risk Insurance Policies Should Direct the Federal Response al Response to Rising Data Breaches", *Washington Journal of Law and Polic*y 40, 7: 257-277. https://core.ac.uk/download/pdf/233188181.pdf.
- Bulgaria. 2016. *Национална стратегия за киберсигурност „Киберустойчива България 2020"* [National cyber security strategy. Cyber resilient Bulgaria 2020]. http://www.cyberbg.eu/doc/20161024_Cyber_strat_proekt.pdf
- Buzan, Barry.1991. "New Patterns of Global Security in the Twenty-First Century". *International Affairs*. Royal Institute of International Affairs 1944-) 67, no. 3: 431-451. https://doi.org/10.2307/2621945.
- Canada. 2018. *National Cyber Security Strategy Canada's Vision for Security and Prosperity in the Digital Age*. https://www.publicsafety.gc.ca/cnt/rsrcs /pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf.
- Carr, Madeline. 2016. "Public–private partnerships in national cyber-security strategies." *International Affairs* 92, 1: 43-62.https://doi.org/10.1111 /1468-2346.12504.
- Caruson, Kiki, Susan A. MacManus, and Brian D. McPhee. 2012. "Cybersecurity PolicyMaking at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success". *Journal of Homeland Security and Emergency Management* 9, no. 2: 1-22. https://doi.org/10.1515/jhsem-2012-0003.
- Cavelty, Myriam Dunn, and Elgin M. Brunner. 2007. "Introduction: information, power, and security—an outline of debates and implications", in Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel,

eds, *Power and security in the information age: investigating the role of the state in cyberspace*. Aldershot: Ashgate.

- Cavelty, Myriam Dunn, and Manuel Suter.2009. "Public–private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection". *International Journal of Critical Infrastructure Protection* 2, 4: 179-187.
- Croatia. 2015. *The National Cyber Security Strategy of The Republic opf Croatia.* https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.
- Czech Republic. 2018. *Cyber Defence Strategy of the Czech Republic 2018–2022*. https://www.vzcr.cz/uploads/69-Cyber-Defence-Strategy-2018.pdf.
- Denmark. 2018. *Danish Cyber and Information Security Strategy 2018-2021*. https://en.fm.dk/media/15468/danishcyberandinformationsecuritystrategy_weba.pdf.
- Ducaru, Sorin. 2016. "The cyber dimension of modern hybrid warfare and its relevance for NATO." *Europolity-Continuity and Change in European Governance* 10, (1): 7-23. https://europolity.eu/wp-content/uploads/2016/07/Vol.-10.-No.-1.-2016-editat.7-23.pdf
- Ducaru, Sorin. 2017. "The security of critical energy infrastructure in the age of multiple attack vectors: NATO's multi-faceted approach." *Europolity-Continuity and Change in European Governance* 11, 1: 5-20. https://europolity.eu/wp-content/uploads/2017/06/Europolity_vol.11_no.1_-2017_art01_Ducaru.pdf.
- ENISA's official website, *National Cyber Security Strategies - Interactive Map* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Italy
- Estonia. *Cybersecurity Strategy Republic of Estonia 2019 2022*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia.
- European Union External Action's website. 2022. Article 42(7) TEU - The EU's mutual assistance clause (accessed on 12 September 2023). https://www.eeas.europa.eu/eeas/article-427-teu-eus-mutual-assistance-clause_en.
- Fjäder, Christian. 2014. "The nation-state, national security and resilience in the age of globalization." *Resilience: International Policies Practices and Discourses* 2, no. 2: 114-129. https://doi.org/10.1080/21693293.2014.914771

- Fidler, David. 2011. "Was Stuxnet an Act of War? Decoding a Cyberattack". *IEEE Security & Privacy* 9, no. 4: 56-59. DOI: 10.1109/MSP.2011.96.
- Finland. 2019. *Finland´s Cyber security Strategy 2019*. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf.
- Fischerkeller, Michael, and Richard Harknett. 2017. "Deterrence is not a credible strategy for cyberspace." *Orbis* 61, 3: 381-393. https://doi.org/10.1016/j.orbis.2017.05.003.
- France. 2015. *French National Digital Security Strategy*. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf.
- Germany. 2021. *Cyber Security Strategy for Germany 2021.* https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=9CB9A479E1496EA1F994129BB137F3D5.live892?__blob=publicationFile&v=4.
- Greece. 2020. *National Cybersecurity Strategy 2020 - 2025.* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece.
- Hungary. 2018. *Government Decision 1838/2018 (XII.28.) on the Strategy for the security of network and information systems in Hungary.* https://nki.gov.hu/wp-content/uploads/2020/11/Strategy-for-the-security-of-network-and-information-systems-in-Hungary.pdf.
- Iceland. 2022. *Icelandic National Cybersecurity Strategy 2022 - 2037*. https://www.stjornarradid.is/library/04-Raduneytin/Haskola---idnadar--og-nyskopunarraduneytid/Icelandic%20National%20Cybersecurity%20Strategy%202022-2037.pdf.
- Italy. 2022. *National Cybersecurity Strategy 2022 - 2026*. https://www.acn.gov.it/ACN_EN_Strategia.pdf.
- Jibilian, Isabella and Katie Canales. 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". *Business Inside*. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cybersecurity-2020-12.

- Junio, Timothy. 2013. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate". *Journal of Strategic Studies*. 36, 1: 125-133. DOI: 10.1080/01402390.2012.739561.
- Kello, Lucas. 2017. *The virtual weapon and international order*. Yale University Press.
- Koch, Robert, and Mario Golling. 2018. The cyber decade: Cyber defence at a X-ing Point. *10th International Conference on Cyber Conflict*. http://dx.doi.org/10.23919/CYCON.2018.8405016.
- Latvia. 2023. *The Cybersecurity Strategy of Latvia 2023 - 2026*. https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf.
- Lilli, Eugenio. 2021. "Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence". *Contemporary Security Policy* 42, 2: 163-188. DOI: 10.1080/13523260.2021.1882812.
- Lindsay, Jon; Gartzke, Erik. 2019. *Cross-domain deterrence: Strategy in an Era of complexity*. Oxford University Press.
- Lithuania. 2018. *Government of the Republic of Lithuania Resolution on the Approval of the National Cyber Security Strategy*. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/27107170d04511e8a82fc67610e51066?jfwid=dg8d31595.
- Lupovici, Amir. 2016. "The "attribution Problem" and the social construction of "violence": taking cyber deterrence literature a step forward". *International Studies Perspectives* 17, 3: 322-342. https://doi.org/10.1111/insp.12082.
- Luxembourg. 2021. *Luxembourg Cyber Defence Strategy*. https://defense.gouvernement.lu/dam-assets/la-defense/Luxembourg-Cyber-Defence-Strategy.pdf.
- Mattei, Tobias. 2017. "Privacy, Confidentiality and Security of Healthcare Information: Lessons from the Recent WannaCry Cyberattack". *World Neurosurgery* 104: 972-974. 10.1016/j.wneu.2017.06.104.
- McGraw, Gary. 2013. "Cyber War is Inevitable (Unless We Build Security In)". *Journal of Strategic Studies* 36, 1:109-119. DOI: 10.1080/01402390.2012.742013.
- Montenegro. 2017. *Cybersecurity strategy of Montenegro 2018- 2021*. https://afyonluoglu.org/PublicWebFiles/strategies/Europe/Montenegro%202018-%202021%20National%20Cyber%20Security%20Strategy-EN.pdf.

- Morgan, Steve. 2023. "Top 10 Cybersecurity Predictions and Statistics For 2023". *Cybercrime Magazine*. https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/.
- Morse, Amyas. 2017. "Investigation: WannaCry cyber attack and the NHS, National Audit Office". *National Audit Office*. https://www.nao.org.uk/wp content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.
- NATO. 2002. *Prague Summit Declaration*. https://www.nato.int/cps/en/natohq/official_texts_19552.htm.
- NATO. 2016. *Warsaw Summit Communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
- NATO's official website. 2023. *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm#defence.
- NATO's official website. 2023. *Resilience, civil preparedness and Article 3*. https://www.nato.int/cps/en/natohq/topics_132722.htm
- NATO's official website. *NATO Industry Cyber Partnership.* https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html.
- Netherlands. 2022. *Netherlands Cybersecurity Strategy 2022-2028. Ambitions and actions for a digitally secure society*. https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028/documents/publications/2022/12/06/the-netherlands-cybersecurity-strategy-2022-2028.
- Norway. 2018. *National Cyber Security Strategy for Norway*. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf.
- Nye Jr., and Joseph Samuel. 2017. "Deterrence and Dissuasion in Cyberspace". *International Security* 41, no. 3: 44–71.
- Poland. 2019. *Cybersecurity Strategy of the Republic of Poland For 2019 – 2024*. https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/poland-cybersecurity-strategy-republic-poland-2019.
- Portugal. 2019. *National Strategy For Cyberspace Security 2019-2023*. Resolution of the Council of Ministers No. 92/2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/portuguese-ncss/@@download_version/ae00f93801664a57b22f9f5f96c1cd01/file_en.

- Ottis, Rain. 2018. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective", *NATO Cooperative Cyber Defence Centre of Excellence*. https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.
- Republic of Macedonia. 2018. *Republic of Macedonia National Cyber Security Strategy 2018- 2022*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/NS%20Cyber%20Security%202018-2022_ENG.pdf
- Rid, Thomas. 2012. "Cyber War Will Not Take Place". *Journal of Strategic Studies* 35, 1: 5-32. http://www.creativante.com.br/download/Cyber%20War.pdf.
- Romania. 2022. *Strategia de securitate cibernetică a României pentru perioada 2022-2027* [Romania's cybersecurity strategy for 2022-2027]. Decision no. 1.321/2021. https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128.
- Slovakia. 2021. *The National Cyber Security Strategy 2021-2025*. https://www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf.
- Slovenia. 2016. *Cyber Security Strategy Establishing a System to Ensure a High Level of Cyber Security*. https://www.gov.si/assets/ministrstva/MDP/DID/Cyber_Security_Strategy_Slovenia.pdf.
- Spain. 2019. *National Cybersecurity Strategy.* https://www.dsn.gob.es/eu/file/2989/download?token=EuVy2lNr.
- Stone, John. 2013. "Cyber War Will Take Place!". *Journal of Strategic Studies* 36, 1: 101-108. DOI: 10.1080/01402390.2012.730485.
- Svitkováa, Katarína. 2017. "Resilience in the National Security Discourse." *Obrana a Strategie* 1: 21-42. 10.3849/1802-7199.17.2017.01.021-042.
- Turkey. 2020. *National Cybersecurity Strategy 2020-2023*. https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf.
- United Kingdom. 2022. *Government Cyber Security Strategy. Building a cyber resilient public sector 2022 - 2023*. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf.
- United States of America. 2023. *National Cybersecurity Strategy*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

- Valeriano, Brandon, and Benjamin Jensen. 2019. "The Myth of the cyber offense." *CATO Institute*, Policy Analysis No. 862, https://www.cato.org/policy-analysis/myth-cyber-offense-case-restraint.
- Walker, Brian, and David Salt. 2006. *Resilience Thinking: Sustaining Ecosystems and People in a Changing World*. London: Island Press.
- Weber, Max.1918. *Politics As a Vocation*. Munich: Munich University.