Finabel

Food for thought 12-2021

Cybersecurity and the European Defence Cooperation

AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Centre

Written by
Maria Vitoria Santana

This Food for Thought paper is a document that gives an initial reflection on the theme. The content is not reflecting the positions of the member states but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. All our studies are available on www.finabel.org

DIRECTOR'S EDITORIAL

The European Union faces a new challenge: how to adapt cyber-security to the European shared defence policy. Developing a common plan to tackle cyber-security is a complex and intricate matter with distinct obstacles on a national and supranational level. On the one hand, from a national point of view, protecting privacy specifically regarding confidential and sensitive information remains the main focus. On the other hand, the European Union has to adapt to Member States' different approaches to cyber-security.

This paper aims to analyse the existent policies and strategies to safeguard European cyber-defence and cooperation in the military field. The pandemic has compelled nations to shift towards an almost complete cyber-existence, and, as with any unexpected change, this brought about questions concerning the safety of data and the weakness of defence in a globalised cybernetic world.

Having a block of countries that abide by the same core rules and act in similar ways when preventing and confronting threats has shaped Europe into a strong, influential, and powerful political actor with a decisive voice in international affairs. This military strategy shall continuously adapt to the new challenges posed by a world that predominately communicates in cyber-space – both nationally and internationally.

Mario Blokken
Director PSec

TABLE OF CONTENTS

Introduction 5

Challenges in Pursuing a Supranational

Cyber Defence Plan. 6
- Legal and Economic Restrictions. 6
- International Threats. 8
- Estonia Cyberattacks 2007. 8
  - Ukraine Cyber Crisis 2014. 9
  - Covid-19 Cyber Crisis 2020 10

NATO and EU Partnership on Defence and Mitigating Cyberthreats. 11
- NATO-EU Cybersecurity Defence Policy (CSDP). 11
- Cyber Defence Pledge. 13

European Military Cyber Resilience. 14
- EU Cybersecurity Strategy. 14
- European Cybersecurity Certification Framework. 15
- NIS Directive. 16

Conclusion 16

Bibliography 17

INTRODUCTION

In a digital world, the hybrid attack has become a recurrent occurrence. To be prepared to fight cyber threats, the European Union (EU) had first to understand this new form of attack and how dangerous it could be. After the Estonian cyberattack of 2007, the need for a response plan able to satisfy national and European defence expectations brought the debate of cybersecurity to the centre of defence and security policies. The technological advances brought by the internet and electronic devices have become a fundamental part of our daily lives. These technological changes have transformed the way we communicate today and have directly impacted how countries handle defence and security strategies.

To tackle cybercrimes and cyberattacks, a strong, defined, and elaborate cyber-secure Europe needs to understand the primary forms of cyber threats and foresee the new trends that emerge from cyberspace. The latter has proven to be a Homeric task. In contrast, cybercrime evolves daily as state and non-state actors actively invest time and money to explore new or pre-existing gaps in digital systems around the globe. Knowledge is key to fighting a cyberwar. With that in mind, the EU plans to defeat those threats by creating research centres, investing in highly qualified professionals, and spreading digital literacy among Member States (MS). The most common forms of attack are Advanced Persistent Threats (APTs), sophisticated attacks operated by hackers that monitor data for long periods to store and steal sensitive information for cyberespionage. These threats account for one-quarter of all cyberattacks.[1]

This paper is divided into three main chapters. The opening chapter, 'Challenges in Pursing a Supranational Cyber Defence Plan', first explores the main legal and economic discussion surrounding cybersecurity and, second, the ground-breaking cyberattacks and crises in Europe. Thus, the Estonian cyberattack of 2007, the Ukraine cyber crisis of 2014, and the Covid-19 cyber crisis of 2020 are explored in an attempt to trace the lessons learned from past mistakes and corroborate that there is a necessity for preparing a plan of action in cases of cyberthreats. In the second chapter, 'NATO and EU Partnership on Defence and Mitigating Cyberthreats', two joint cybersecurity initiatives are analysed: the NATO-EU Cybersecurity Defence Policy (ESDP) and the Cyber Defence Pledge. This chapter also tackles the improvement of each of their prospects as well as their expected results. The final main chapter, 'European Military Cyber Resilience', debates the military strategies on the fight against cyberthreats. This paper focuses on the EU Cybersecurity Strategy, the European Cybersecurity Certification Framework, the Cybersecurity Act, and the NIS Directive. Moreover, this work will also consider, through a military lens, the outcomes and the financial, legal, and social expectancies of the Member States and the EU. The main fo-

1. European Court of Auditors Briefing paper, "Challenges to effective EU cybersecurity policy" March 2019 [online]. Available at https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

cus of this paper is to understand the military strategies drafted to prevent cyberattacks by analysing past cyber crises and some of the EU proposals for enhancing cybersecurity.

CHALLENGES IN PURSUING A SUPRANATIONAL CYBER DEFENCE PLAN.

Achieving a supranational cyber defence plan is an arduous task. It involves legal and economic powers from a national and international perspective, which has been part of the EU plans for more than two decades now. Repeated cyber crises have exposed the digital weak points of both Member States and the European Union, thus highlighting the necessity to adapt to a digital world from a security point of view

Legal and Economic Restrictions.

One of the main problems of tracing a common strategy was establishing a common legal approach to cybersecurity that would satisfy the needs of all countries. The Budapest Convention of Cybercrime of 2000 was the first European treaty to address legal violations on the internet or other shared computer networks. This treaty considered copyrights violations, computer-related fraud, child pornography, and network security violations exclusively. With new cyber threats, the legislation was forced to adapt the 2013 cybersecurity strategy and the 2016 Network and Information Security (NIS) into common European legislation on cybersecurity. The 2018 directive, aiming to set a harmonised level of legal capabilities, was drafted by urging the Member States to endorse the NIS strategies while pursuing national single points of contact and computer security incident response teams (CSIRTs) by defying the mandatory rules for digital essential services and critical information.[2]

In 2015, the Digital Single Market Strategy was presented. In May and in April of the same year, the European Agenda on Security adopted the fight against cybercrime as one of the three pillars of the 2015 Agenda, along with tackling terrorism, preventing radicalisation, and disrupting organised crime. In 2016 the Commission included special measures aiming to boost the cybersecurity industry and to fight cyber threats. Figure 1 provides a visual explanation of the legislation in October 2021.

European international laws are based on State sovereignty, and the same concept applies to the cyber legislative framework that encompasses every individual national law to create a cybersecurity regulation. While considering cybersecurity and international law, the industry and the private sectors have a crucial role. Indeed, the financial investment from those two actors is fundamental for the cyber development of a country. [3] The legal and financial sectors are allies in cybersecu-

2. Ibid European Court of Auditors Briefing paper, "Challenges to effective EU cybersecurity policy"
3. Jan Wouters & Anne Verhelst. Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives International Organisations Research Journal (2020). [online]. Available at: 10.17323/1996-7845-2020-02-07.

Table 1 – Gaps and uneven transposition in the legislative framework (non-exhaustive)

Policy area	Examples
Digital Single Market	o The present Consumer Sales Directive does not cover cybersecurity. The proposed directives on digital content[47] and online sales[48] aim to address this gap. o There are limited and diverse legal frameworks for duties of care in EU Member States, giving rise to legal uncertainty and difficulty in enforcing legal remedies[49]. o Policies on software vulnerability disclosures are being developed at different speeds across Member States, with no overarching legal framework at the EU level to enable a coordinated approach[50].
Strengthening network and information security	o Member States are free to include sectors omitted from the NIS Directive[51]. The accommodation industries, which are not covered, can be a gateway for other crimes, including human and drug trafficking and illegal immigration[52].
Fighting cybercrime	o Many Member States have not defined e-evidence in their national legislation[53] (see also paragraph 22). o The current framework decision on non-cash payment fraud does not explicitly include non-physical payment instruments such as virtual currencies, e-money and mobile money, nor does it cover such acts as phishing, skimming and the possession and sharing of payer information[54]. o The Directive on Attacks against Information Systems does not directly address illegal data acquisition from the inside (e.g. cyberespionage), leading to challenges for law enforcement[55]. o In the wake of the Court of Justice of the European Union judgment on data retention[56], differences in the application of the legal framework among Member States has impeded law enforcement, potentially resulting in the loss of investigative leads and impairing effective prosecution of online criminal activity[57].

Source: ECA.

Source: Stockvault, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

Figure 1 : Gap and uneven transposition in the legislative framework,
Challenges for an effective Cybersecurity plan, March,2019

rity as they are primarily dependant on one another to secure Europe in its fight against cyberthreats.

The funding challenges of a common European cybersecurity plan concern both state and non-state actors. European investment in cybersecurity is estimated between 1 billion and 2 billion euros per year.[4] There is no obligation for the Member States to lay out separate financial plans covering cybersecurity, making it difficult for the EU to assess how state and private actors support the advancement of cybersecurity. Nevertheless, an initial public investment relying on private investors after implementation tends to be the most used economic strategy.[5] The lack of sufficiently patented results EU's research and innovation sector prevents Europe from achieving the desired level of competitiveness and digital autonomy, which motivated the Commission to establish a network of cybersecurity competence centres and research competence centres to boost the cybersecurity research field and investments.

In the period from 2014 to 2018, the Commission spent at least 1.4 billion euros implementing the Strategy, allocating the largest share to the research and innovation programme, Horizon 2020,[6] which has cybersecurity and cyberprivacy as a common component of the two streams of the programme: the "Secure societies – Protection freedom and security of Europe and its citizens" and the "Fighting Crime and Terrorism" – the latter with a particular focus on cyberterrorism and privacy attacks[7].

International Threats.

There has been several cyberattacks and crises in the past few years in Europe. However, three of them have significantly impacted how the EU handles the matter of cybersecurity: the Estonian cyberattacks of 2007, the Ukraine cyber crisis of 2014, and, more recently, the Covid-19 cyber crisis. To understand how they have forged today's European cyber panorama, it is necessary first to establish how and why they happened and what lessons were learned in each case.

Estonia Cyberattacks 2007.

The cyberattack that shaped Estonia's digital approach and transformed the country into a cybersecurity 'hotshot' was a political retaliation attributed to a Russian IP address to the Estonian governmental decision of moving the Bronze Soldier statue from the centre of Tallinn to a military cemetery on the periphery of the city. The statue portrays a soldier bowing his head and wearing a World War II (WWII) Red Army uniform. It was built during the Russian occupation of Estonia and was originally called "Monument to the Liberators of Tallinn".[8] The statue carries a controversial meaning for Estonians. While the Russian speaking citizens consider it to represent the USSR victory over Nazism, the ethnic Estonians view it as a symbol of the Soviet oppression endured for half a century.[9]

4. Ibid European Court of Auditors Briefing paper, "Challenges to effective EU cybersecurity policy"
5. Ibid
6. Ibid
7. European Commission Fact sheet " EU cybersecurity - Initiatives working towards a more secure online environment" January 2017 p6 [online]. Available at https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf
8. **Damien McGuinness** "How a cyber attack transformed Estonia" BBC News, 27 April 2017 Tallinn, Estonia, [online]. Available at: https://www.bbc.com/news/39655415
9. Ibid Damien McGuinness " How a cyber attack transformed Estonia"

When considering both parties, the Estonian authorities decided to move the statue to a more secluded area where the Russian-speaking Estonians could pay their respects while assuring that ethnic Estonians would not have such a symbol in the centre of Tallinn. When the authorities announced the decision in April 2007, a horde of Russian-speaking Estonian protesters occupied the streets and made false claims saying that the statue and some Soviet war graves would be destroyed. These protests caught the attention of some Soviet activists, who then sieged Estonian cyberspace.[10]

The cyberattacks lasted for twenty-two days from 27 April 2007 to 18 May 2007. They resulted in a temporary degradation and loss of service in both governmental and commercial websites, as well as access to banks and emails. The attacks came mainly from offshore IP addresses that led to banks cutting off all foreign transactions. The instruction for the attacks was propagated in Russian web forums and other websites where users explained, in Russian, which of the Denial of Services (DoS) or Distributed Denial of Service (DDoS) methods should be used as well as when the attacks should happen. As for cyber violations, the predominant ones during this operation were: ping flood (when the attacker takes down a victim's computer by overflowing it with ICMP echo requests, also known as pings[11]), UDP flood (a kind of Denial of Service [DoS] attack in which the attacker overflows random ports on the targeted host with IP packets containing UDP datagrams[12]), malformed web queries, and email spam that drew the receiver's attention on a link that generates the cyber access for the attackers[13].

What could have resulted in discrediting the government's ability to secure their digital rights and presence from this new form of threat quickly evolved into a relationship of trust built upon the efficiency with which the government, with support from NATO and other nations, responded to the incident. Using the national autonomy power, Estonia denied access to financial services from outshore transactions and isolated the country database from international activities. As such, it was able to counter the economic and privacy damage posed by the attack.[14]

Ukraine Cyber Crisis 2014.

As the relationship between Kyiv and Moscow collapsed in 2014 due to Russia's annexation of Crimea and the eastern Ukrainian pro-Russian separatist movement going against the ceasefire agreement, Ukraine became the target of various cyberattacks in December. Former President Petro Poroshenko referred to this attack as a cyberwar.[15] The 6,500 cyberattacks lasted for two months and targeted finance and defence ministries. The Kyiv blackouts resulting from a hack attack on the city's power grid were also attributed to Russia. The 2014 blackout was the first to occur; however, the 2016 blackout was the most

10. Ibid
11. Ping flood (ICMP flood), Imperva, [online] https://www.imperva.com/learn/ddos/ping-icmp-flood/
12. UDP Flood, Imperva, [online] https://www.imperva.com/learn/ddos/udp-flood/
13. Rain Ottis "Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective" Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited, pp 163-168, [online]. Available at: https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/
14. Sean Aday et al. Hybrid Threats. "Hybrid Threats: 2007 cyber attacks on Estonia" A Strategic Communications Perspective. Riga: NATO Strategic Communications Centre of Excellence (2019) [online]. Available at: https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86
15. Natalia Zinets " Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar' Reuters, 29 December 2016, , [online]. Available at: https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC

effective as it lasted for six hours and affected around 230,000 Ukrainians.[16]

The attack on the State Treasury incapacitated the systems for several days, effectively preventing all state workers and pensioners from receiving their salaries and social benefits on time. A cyber security firm called CrowdStrike attributes the implantation of malware on Android devices, one of the access points to Ukrainian digital systems,[17] to a group connected to the Russian government. This incident was reported by specialists as the first cyberwar episode[18] and supported President Poroshenko's initial claims. Thus, while Ukraine's security council did not disclose the measures taken to rectify the situation, the country has become one of the leading names in the fight against cybercrimes.

Other than the financial and security violations, the attacks also disabled parts of the Ukrainian election network system three days before the presidential election in May 2014 by using an advanced cyberespionage malware, according to the International Foundation of Electoral Systems.[19] The same also happened in October before the parliamentary election. Ukraine's Security Service (SBU) managed to discover the malware in the system of the Central Election Commission ahead of the election day, ensuring that the results were not fraudulent. The Russian hacker group Cyber Berkut claimed responsibility for this attack.[20] The attacks reveal the importance of investing in cybersecurity by having a qualified person that can track and stop malware and other cyber invasions in time. After the crisis, the Ukrainian government invested in having a more efficient cyber response. This initiative was also supported by the United States (US) and other European and non-European intelligence agencies. Washington is one of the most prominent investors in the Ukraine cybersecurity intelligence program. It is estimated that the US alone invested more than 8.9 million euros. This investment has proved to be fruitful, vide Dmytro Shymkiv's, the former Ukraine chief cyber adviser, statement: "Some of the viruses and malware in the energy blackouts in Ukraine were later found in the US and Israel".[21] In cyber defence, one of the biggest assets is being able to prevent a crisis from happening, which requires a well-prepared, intelligent plan of action.

Covid-19 Cyber Crisis 2020

Unlike the other two cyberattacks previously explored in this paper, the Covid-19 cyber crisis did not start as a personal attack on any nation or government. The isolation and social-distancing measures enforced worldwide forced entire national systems to shift quickly to online platforms. These unexpected transformations have exposed the cybersecurity gaps and the digital illiteracy levels[22] of state workers who were neither prepared nor cor-

16. Laurens Cerulus "How Ukraine became a test bed for cyberweaponry" Politico EU, 14 February 2019, [online]. Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/
17. Ibid Natalia Zinets " Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'"
18. Ibid.
19. Laurens Cerulus "How Ukraine became a test bed for cyberweaponry" Politico EU, 14 February 2019, [online]. Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/
20. Tim Maurer, "Cyber Proxies and the Crisis in Ukraine" ed Cyber War in Perspective: Russian Aggression against Ukraine" Kenneth Geers, ed. (NATO CCD COE Publications, Tallinn 2015). 79-86
21. Ibid Laurens Cerulus "How Ukraine became a test bed for cyberweaponry".
22. European Court of Auditors review 02 "EU actions to address low digital skills" 2021 [online]. Available at https://www.eca.europa.eu/Lists/ECADocuments/RW21_02/RW_Digital_skills_EN.pdf

rectly instructed to behave digitally in their home office.[23]

The use of a personal computer to access official accounts and the use of state devices to log into personal accounts and research allowed hackers to plant malware links that allowed them to infiltrate into national archives.[24] One of the most commonly used strategies was to generate a website that looked trustworthy with regard to Covid-19 information.[25] Although some spoke of a cyber pandemic,[26] a possibility that has yet to be completely overruled,[27] the Covid-19 cyber crisis was rooted mainly in the lack of digital literacy and a structured state cyber presence rather than being an epidemical attack against national systems worldwide[28].

Nevertheless, the EU did not overlook this exposure, which drafted the 'New EU Cybersecurity Strategy'[29] to enhance the EU command on international supranational and national rules and standards within cyberspace. To do so, strong international cooperation among the Member states is essential. Developing a single European approach ensures that it will be grounded in the rule of law, human and fundamental rights, and will be used to enhance democratic values.[30]

NATO AND EU PARTNERSHIP ON DEFENCE AND MITIGATING CYBERTHREATS.

NATO and the EU are strong allies when it comes to defence and security policies. This alliance has proven to be crucial on several occasions. Indeed, when navigating the digital waters, the opportunity to learn with other Alliance members, more specifically with the United States, is extremely valuable. The current defence policies and agreements were adapted to serve the purpose of guaranteeing European security in cyberspace.

NATO-EU Cybersecurity Defence Policy (CSDP).

In 2013, the European Union and NATO decided that cyberspace defence laws and norms should abide by the same legal framework defined by the European Security and Defence Policy (ESDP). The European Military concept of securing MS and its citizens was extended to the cyber reality that abides by the existing Military regulations and aims to enhance European cyberspace and cyber auton-

23. Ibid European Court of Auditors review 02 "EU actions to address low digital skills"
24. Daniel Lohrmann 'How Is Covid-19 Creating Data Breaches?' Govtech 29 March, 2020 [online] Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-is-covid-19-creating-data-breaches.html
25. Ibid Daniel Lohrmann 'How Is Covid-19 Creating Data Breaches?'
26. Daniel Lohrmann '2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic' Govtech, 11 December 2020 [online]. Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html
27. Ibid Daniel Lohrmann '2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic'
28. Ibid
29. European Commission 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient' 16 December 2020[online]. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
30. Ibid European Commission 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient' 16 December 2020[online].

THREAT ORIGIN	THREAT LEVEL	CHARACTERISTIC	TIER	DEFINITION
CYBERDOMAIN	A	Exploits pre-existing known vulnerabilities	1	**Practitioners** who rely on others to develop the malicious code, delivery mechanisms and execution strategy (use known exploits).
			2	**Practitioners** with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).
	B	Discovers unknown vulnerabilities	3	**Practitioners** who focus on the discovery and use of unknown malicious code are adept at installing user and kernel mode root kits ([35]), frequently use data mining tools and target corporate executives and key users (government and industry) for the purpose of stealing personal and corporate data with the expressed purpose of selling the information to other criminal elements.
			4	**Criminal** or **state actors** who are organised, highly technical, proficient, well-funded professionals working in teams to discover new vulnerabilities and develop exploits.
	C	Creates vulnerabilities using full spectrum	5	**State actors** who create vulnerabilities through an active programme to 'influence' commercial products and services during design, development or manufacturing, or with the ability to impact products while in the supply chain to enable exploitation of networks and systems of interest.
			6	**States** with the ability to successfully execute full spectrum (cybercapabilities in combination with all of their military and intelligence capabilities) operations to achieve a specific outcome in political, military, economic etc. domains and apply at scale.

Source: Stockvault, http://publications.europa.eu/resource/cellar/2e35913c-1d03-11e8-ac73-01aa75ed71a1.0001.01/DOC_1

Table 2: Cyberthreat taxonomy (US DoD Defence Science Board Report, 2013)

Figure 2: European Parliament 'Cyberthreat taxonomy' Cybersecurity in the EU Common Security and Defence Policy (CSDP),

Challenges and risks for the EU, May,2017

omy while assuring peace and stability amidst the states and providing a secure environment in the digital sphere.[31]

The European cyberspace is a shared domain that relies upon the concepts of supranational security to guarantee national privacy, self-governance, and command of control systems on the common agreement to enhance information exchange, international support for cyber development, and the efficiency of this new shared environment[32].

Cyberthreats can be divided into three different levels according to the ways in which the vulnerabilities are exploited. Figure 2 provides a visual understanding of how the EU and NATO have defined those threats.[33] The CSDP was drafted to provide a common solution to each one. However, to respond efficiently to these new hybrid threats, it is essential to endorse a shared effort to enhance European cyberspace, a substantial investment from state and non-state actors on research in the field, and common best practises regarding digital exchanges.

Cyber Defence Pledge.

NATO's Cyber Defence Pledge was adopted at the NATO Summit in Warsaw in 2016. The pledge consists of seven NATO obligations, listed below, which aim to ensure a secure cyberspace for NATO nations.

> "I. Develop the fullest range of capabilities to defend our national infrastructures and networks. This includes: addressing cyber defence at the highest strategic level within our defence related organisations, further integrating cyber defence into operations and extending coverage to deployable networks;
> II. Allocate adequate resources nationally to strengthen our cyber defence capabilities;
> III. Reinforce the interaction amongst our respective national cyber defence stakeholders to deepen cooperation and the exchange of best practices;
> IV. Improve our understanding of cyber threats, including the sharing of information and assessments;
> V. Enhance skills and awareness**,** among all defence stakeholders at the national level, of fundamental cyber hygiene through to the most sophisticated and robust cyber defences;
> VI. Foster cyber education, training and exercising of our forces, and enhance our educational institutions, to build trust and knowledge across the Alliance;
> VII. Expedite implementation of agreed cyber defence commitments including for those national systems upon which NATO depends."[34]

These obligations set the rules as to which agreements regarding cybersecurity will be drafted. Considering NATO defence and security policies, this is especially important to the EU since most international EU defence agreements abide by NATO rules and laws. NATO's cyber defence pledge is also the next step towards fulfilling the NATO cyber de-

31. European Parliament 'Cybersecurity in the EU Common Security and Defence Policy (CSDP), Challenges and risks for the EU', May,2017 [online]. Available at : http://publications.europa.eu/resource/cellar/2e35913c-1d03-11e8-ac73-01aa75ed71a1.0001.01/DOC_1
32. Ibid European Parliament 'Cybersecurity in the EU Common Security and Defence Policy (CSDP), Challenges and risks for the EU'
33. Ibid
34. NATO Official texts ' Cyber Defence Pledge' 08 July 2016 [online]. Available at https://www.nato.int/cps/en/natohq/official_texts_133177.htm

fence policy endorsed at the Wales Summit of 2014. Incentivised by the common goal of building a stronger common cyber defence, the pledge represents NATO cooperative proposals amidst nations and private and state actors.

The pledge reinforces that the main priority of NATO's cyber defence policy is protecting data, information, and system operation within the Alliance. The framework of cyber defence expansion and the response for cyber-attacks are the backbone of the police and the pledge. Furthermore, investing in education and encouraging digital literacy among civilians and state citizens is crucial to enhancing the security level in the Alliance cyberspace.

The pledge also represents NATO's recognition of cyberspace as an operational domain endowed with the same importance as land, air, and sea. In so doing, the core values and policies that apply to NATO defence agreements and international legal operations are also applicable in cyberspace. Therefore, the national efforts regarding security in the international Alliance arena now have a fourth front to consider cyberspace.

EUROPEAN MILITARY CYBER RESILIENCE.

Cyberspace is now one of the fronts on which Europe joint efforts operate to assure the safety of its citizens, their privacy, as well as their data. Furthermore, it also secures delicate national and international information. Privacy is only one of the main issues regarding the cyber domain. In a world constantly more connected, having access to a national digital system entails controlling banks' national systems, electoral portals, and other fundamental operational organisations responsible for the country's proper functioning.

EU Cybersecurity Strategy.

Regarding its Cybersecurity Strategy, the EU's main goal is to guarantee safe and open access to the internet while ensuring that the European values and fundamental rights are being respected. On those bases, the strategy has three main areas of action: resilience, technological sovereignty, and leadership; building operation capability to prevent, deter, and respond; and advancing **a global and open cyberspace through increased cooperation.**[35]

The Commission proposes the first point of action, resilience, technological sovereignty, and leadership**, with a Directive on the measures for a higher level of joint cybersecurity within the Union by revising the NIS Directive to enhance cyber resilience levels in both private and public sectors.**[36] **Moreover, the Commission also proposes a network of Security Operations Centres that will work across Europe, empowering**

35. European Commission 'The Cybersecurity Strategy' 29 September 2021 [online]. Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

36. European Commission Press Release 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient' 16 December 2020 [online]. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

Artificial Intelligence (AI) and its ability to shield Europe from cyberattacks. The Digital Innovation Hubs, additional measures to support small and medium-sized businesses (SMEs), were designed to attract investments and an exchange of professional skills, enlarge research efforts, and boost innovation in the sector.

The second area of action, building operation capability to prevent, deter, and respond**, has elicited a new Joint Cyber Unit that aims to strengthen the cooperation between MS and EU bodies responsible for preventing, deterring, and responding to cyberattacks.[37] The efforts are to be carried out on a national and European scale with the support of the European Defence Agency and the European Defence Fund.**

The third area of action, advancing **a global and open cyberspace through increased cooperation, aims to build stronger rules based on the global order, while promoting international security and stability within cyberspace.[38] The protection of human rights and fundamental freedoms is also a core concern. A healthy cyber exchange and dialogue with third-world countries rely on Cyber diplomacy behaviours.**

European Cybersecurity Certification Framework.

The European Cybersecurity Certification Framework consists in a certificate that a product, service or digital system is secured according to the European Cyber defence standards. There are different ICT schemes for securing digital products in the EU, and this certification attests that the products approved abide by the European rules. The certificate also attests to the following: the categories of products and services covered meet the cybersecurity requirements according to which the product was evaluated and the intended level of assurance.[39]

The certificate standardises the security levels for digital products and informs users of the possible risks that, according to the certificate, are described as basic, substantial, or high. These risks are measured by weighing the impacts of a possible attack on leaking personal data or allowing a hacker to access a device.[40]

Cybersecurity Act.

In September 2017, the European Commission presented a proposal that came to be Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity), a complementary regulation to Regulation (EU) No 526/2013 (Cybersecurity Act).

The Cybersecurity Act was a response to the decision-making powers newly granted to the European Union Agency for Cybersecurity (*ENISA*)[41] that boosted the public-private partnership on Cybersecurity that, in 2016, started to discuss the basis for the Cybersecurity certification framework, based on the

37. Ibid European Commission Press Release 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient'
38. Ibid
39. European Commission Shaping Europe's digital future 'The EU cybersecurity certification framework' 1July 2021[online]. Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

40. Ibid European Commission Shaping Europe's digital future 'The EU cybersecurity certification framework'
41. European Commission Press Release 'The EU Cybersecurity Act enters into force
'27 July 2019[online]. Available at http://www.ecs-org.eu/newsroom/the-eu-cybersecurity-act-enters-into-force

Regulation (EU) No 526/2013. The European Cyber Security Organisation (ECSO), a contractual implementation between public-private sectors that has set the rules for how this relationship will take form at the core of this contract, sets out transparency rules and shared efforts to identify relevant cybersecurity gaps in the European digital domain.[42]

NIS Directive.

The first piece of EU legislation implemented in a European totality was the NIS Directive, which provides a legal measure to boost European cybersecurity levels. Its main concerns are MS readiness to respond to a cyberthreat and assuring that they are properly equipped to do so, securing cooperation amidst MS to support and facilitate a strategic exchange of information, and creating a culture of security across the fundamental economic sectors (energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure). These sectors were granted special security measures and communication channels that assure quicker notification to the national authorities.[43]

Article 23 of the NIS Directive requires that the Directive periodically undergoes a functionality review. The 2020 review has proven that NIS was not aligned with the objectives of the Security Union regarding cyber defence expectations. To rectify it, the NIS 2 was presented on 16 December 2020.[44] The goal of the new directive is to adapt to the current needs and prepare for the future, allowing new sectors to participate based upon their economic and societal influence. "The new directive ensures that SME's operating on relevant sectors is included under the NS2 protective measure.[45]

CONCLUSION

Defence and Security Policies are at the heart of the EU joint efforts. With the growing importance of digital communication and cyber presence in the daily lives of citizens and state and private actors, basic system cybersecurity has become a major issue. The first time the EU brought up cybersecurity as a union concern was in 2000, more than two decades after a great deal was accomplished due to the common effort towards a more secure European and global cyberspace.

An important step was acknowledging cyberspace as one of the spaces deserving the same European protection destined for land, force, and air. Nevertheless, cyberspace has peculiarities that cannot be experienced on any other front. The private sector power of influence, both financial and professional, and the dif-

42. Ibid European Commission Press Release 'The EU Cybersecurity Act enters into force'
43. European Commission Shaping Europe's digital future 'NIS Directive' 1 July 2021[online]. Available at https://digital-strategy.ec.europa.eu/en/policies/nis-directive

44. European Commission Shaping Europe's digital future 'NIS Directive' 1 July 2021[online]. Available at https://digital-strategy.ec.europa.eu/en/policies/nis-directive
45. European Commission Shaping Europe's digital future 'Proposal for directive on measures for high common level of cybersecurity across the Union ' 08 March 2021[online]. Available at https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

ferent ways MS invests in cybersecurity and development at national levels have proven to be unique characteristics that permeate the European cyber domain.

Europe is still far from achieving autonomy in cyber security. This is partly due to the different national approaches towards cyberspace and how countries understand security and defence policies in a digital world. Nevertheless, the lack of research projects and initiatives in the sector on both national and European levels places Europe in a disadvantaged position compared to the US, China, or Russia regarding cyber development[46]. Thus, this disparity represents another threat to European cyber sovereignty. As such, the Union is still dependant on the information exchange with other members of the NATO Alliance, especially the U.S., to keep up with the newest cyber defence strategies.

The European cyberspace is built upon human rights, the rule of law, and transparency. It represents European values and Europe's desire to evolve in a more equalitarian and integrative cyberspace than the ones at the top of the cyber security domain. Finding this balance while thriving in a world becoming more cybernetical is perhaps one of the biggest challenges for the European Defence and Security Policy. To address this properly, the EU Cybersecurity Industrial, Technology, and Research Competence Centre (ECCC) agreed in 2020, alongside the MS, on the operational procedures that the ECCC is to follow to enhance European cyber autonomy.

To conclude, the efforts that the EU shares on cybersecurity start long before the cyber battleground. Building a proficient and digital literate European Union is fundamental to prevent hackers from accessing personal data and private and public systems. Educating citizens about common cyber threats can prevent some attacks. However, the ECCC and other research centres around Europe will launch a fundamental education project on giving professionals the ability to venture into the cyber world in search of a more secure, ethical, inclusive, and efficient European cyberspace.

BIBLIOGRAPHY

Aday, Sean, Andžāns Māris, Bērziņa-Čerenkova Una, Granelli Francesca, Gravelines John-Paul, Hills Mils, Holmstrom Miranda, Klus Adam, Martinez-Sanchez Irene, Mattiisen Mariita, Molder Holger, Morakabati Yeganeh, Pamment James, Sari Aurel, Sazonov Vladimir, Simons Gregory and Terra Jonathan. Hybrid Threats. "Hybrid Threats: 2007 Cyber Attacks on Estonia" A Strategic Communications Perspective. Riga: NATO Strategic Communications Centre of Excellence (2019) [online]. Available at: https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86 [Accessed 13 September, 2021].

46. Martio Esteban et al. 'Europe in the Face of US-China Rivalry' European Think-tank Network on China (ETNC) January 2020 [online]. Available at: https://www.egmontinstitute.be/content/uploads/2020/01/2001122-Final-ETNC-report-Europe-in-the-Face-of-US-China-Rivalry.pdf?type=pdf

Bērziņa-Čerenkova Una Aleksandra, Ekman Alice, Esteban Mario, Jerdén Björn, Otero-Iglesias Miguel, Poggetti Lucrezia, Seaman John, Summers Tim, Szczudlik Justyna 'Europe in the Face of US-China Rivalry' European Think-tank Network on China (ETNC) January 2020 [online]. Available at: https://www.egmontinstitute.be/content/uploads/2020/01/200122-Final-ETNC-report-Europe-in-the-Face-of-US-China-Rivalry.pdf?type=pdf[Accessed September 14, 2021].

Cerulus, Laurens "How Ukraine became a test bed for cyberweaponry" Politico EU, 14 February 2019, [online]. Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ [Accessed September 14, 2021].

European Commission 'New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient' 16 December 2020[online]. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 [Accessed 20 September 2021].

European Commission 'The Cybersecurity Strategy' 29 September 2021 [online]. Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy[Accessed 29 September 2021].

European Commission Fact sheet "EU cybersecurity - Initiatives working towards a more secure online environment" January 2017 p6 [online]. Available at https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf [Accessed 11 September 2021].

European Commission Shaping Europe's digital future 'NIS Directive' 1 July 2021[online]. Available at https://digital-strategy.ec.europa.eu/en/policies/nis-directive

European Commission Shaping Europe's digital future 'Proposal for directive on measures for high common level of cybersecurity across the Union' 08 March 2021[online]. Available at https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union[Accessed September 14, 2021].

European Commission Shaping Europe's digital future 'The EU cybersecurity certification framework' 1 July 2021[online]. Available at https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

European Court of Auditors Briefing paper, "Challenges to effective EU cybersecurity policy" March 2019 [online]. Available at https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf [Accessed 4 September 2021].

European Court of Auditors review 02 "EU actions to address low digital skills" 2021 [on-

line]. Available at https://www.eca.europa.eu/Lists/ECADocuments/RW21_02/RW_Digital_skills_EN.pdf [Accessed 20 September 2021].

European Parliament Cybersecurity in the EU Common Security and Defence Policy (CSDP), Challenges and risks for the EU, May 2017 [online]. Available at: http://publications.europa.eu/resource/cellar/2e35913c-1d03-11e8-ac73-01aa75ed71a1.0001.01/DOC_1 [Accessed 14 September 2021].

Lohrmann, Daniel '2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic' Govtech, 11 December 2020 [online]. Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html [Accessed 20 September 2021].

Lohrmann, Daniel 'How Is Covid-19 Creating Data Breaches?' Govtech 29 March, 2020 [online] Available at: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-is-covid-19-creating-data-breaches.html [Accessed 20 September 2021].

Maurer, Tim "Cyber Proxies and the Crisis in Ukraine" ed Cyber War in Perspective: Russian Aggression against Ukraine" Kenneth Geers, ed. 79-86 NATO CCD COE Publications, Tallinn 2015. [Accessed 14 September 2021].

McGuinness, Damien "How a cyberattack transformed Estonia" BBC News, 27 April 2017 Tallinn, Estonia, [online]. Available at: https://www.bbc.com/news/39655415 [Accessed 14 September 2021].

NATO Official texts 'Cyber Defence Pledge' 08 July 2016 [online]. Available at https://www.nato.int/cps/en/natohq/official_texts_133177.htm[Accessed 14 September 2021].

Ottis, Rain "Analysis of the 2007 Cyberattacks against Estonia from the Information Warfare Perspective" Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008. Reading: Academic Publishing Limited, pp 163-168, [online]. Available at: https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/[Accessed 14 September 2021].

Wouters, Jan & Verhelst, Anne. Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives International Organisations Research Journal (2020). [online]. Available at: 10.17323/1996-7845-2020-02-07. [Accessed 4 September 2021].

Zinets, Natalia "Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar' Reuters, 29 December 2016, [online]. Available at: https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC[Accessed 14 September 2021].

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and *ad hoc* coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1 box 44
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 05 – GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at **www.finabel.org**

European Army Interoperability Centre

www.linkedin.com/in/finabelEAIC @FinabelEAIC @FinabelEAIC

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 05