

# **Challenges for cyber defence in the context of Common Security and Defence Policy**

Essay

Created for the CSDP Olympiad 2024  
in Budapest Hungary

Author:

**Officer Cadet Kristof Fischinger**

Student of the Theresan Military Academy  
Austria

Wiener Neustadt, October 2023

## **Abstract**

This essay explores the fast-moving topic of cyber defence in light of the CSDP (Common Security and Defence Policy). As cyber threats jeopardise national security and critical infrastructure, understanding the challenges in cyber defence within the CSDP is crucial. This essay explores these challenges and provides insights to enhance cyber defence capabilities. The research identifies key challenges within the CSDP, like the rapidly evolving threat landscape demands, the lack of standardisation in cyber defence capabilities and limited information sharing hinders proactive cyber defence in the CSDP, and additionally, the shortage of skilled cyber defence professionals and investments in training, education, and in collaborations with industry and academia. The author emphasises the need for increased cyber defence capabilities to mitigate such threats and discusses potential challenges. The essay concludes by emphasising the importance of balancing the need for improved cyber defence with the legal considerations of any actions taken. It also discusses what cyber defence capabilities must be increased and looks more closely at the measures planned to protect the EU (European Union Member States) from cyberattacks. This essay provides insights into cyber defence challenges the CSDP faces, describes actionable recommendations to bolster cyber resilience, protect critical infrastructure, and ensure the EU's security and stability against evolving threats.

## **Keywords**

Common Security and Defence Policy, cyber defence, cyber security, cyber threats, European Union

## 1. Table of Contents

<b>1.</b>	<b>Table of Contents</b> .....	1
<b>2.</b>	<b>Preface</b> .....	2
<b>3.</b>	<b>Introduction</b> .....	3
<b>4.</b>	<b>Current State of Research</b> .....	5
<b>5.</b>	<b>Research Gap</b> .....	7
<b>6.</b>	<b>Research Question</b> .....	8
<b>7.</b>	<b>Methodology</b> .....	9
<b>8.</b>	<b>Research and Results of Research</b> .....	10
8.1	The focal Points of Cyber Defence in the CSDP .....	10
8.2	The Cyber Threats for CSDP .....	11
8.3	The Enhancement of Cyber Defence .....	14
8.3.1	Cooperation and Information Sharing among Member States .....	15
8.3.2	Investment in Cyber Defence Technologies and Training .....	15
<b>9.</b>	<b>Discussion of Results and personal Conclusion</b> .....	17
<b>10.</b>	<b>Annexes</b> .....	19
10.1	List of Abbreviations .....	19
10.2	List of Figures .....	20
10.3	List of Literature .....	21
10.3.1	Books .....	21
10.3.2	Internet .....	22
<b>11.</b>	<b>Affidavit</b> .....	23

## **2. Preface**

The fast-paced digital world has fundamentally changed how people live, work, and communicate. The author follows the rapid development and evolution of technology and computers. Keeping up with the most recent trends and technology advancements in the digital world was and stayed the author's interest. He grew up with more technology than the past generations and kept track of the new technical inventions. Living in a time of high risk of becoming a cybercrime victim, this essay's goals are to explain to the readers the challenges that come with cyber defence within the framework of the CSDP, as well as to give the author a platform to share his opinions and demonstrate his passion for the issue. Although there are advantages of digitisation, it is crucial to be aware of its dangers and difficulties, particularly in cyber security. This essay seeks to add to the cyber security conversation and increase public awareness of a crucial issue. In addition, the author would like to take this opportunity to thank the Chairman of the EU Military Erasmus (EMILYO) Implementation Group, Colonel Assoc. Prof. Hon. Sen. Gell Harald, PhD (habil), MSc, MSD, MBA for the opportunity to participate in the CSDP Olympiad with a topic of his choice.

### 3. Introduction

Cyberattacks are a significant security problem in the modern world, given how interconnected everything is and how much we rely on digital infrastructure. Cyberattacks can limit the functioning of an entire state without ever requiring a soldier to cross a border. Sending the navy, air force, or tanks in return is likely ineffective.

In today's digital age, the growing threat of cyberattacks has become a pressing concern for nations and international organisations. Within the CSDP framework, cyber defence is a critical area that requires careful attention and robust strategies. The CSDP, as an integral part of the European Union's security and defence architecture, faces unique challenges in safeguarding its Member States from cyber threats.

The main contention of this essay is that the CSDP faces significant challenges in preventing cyberattacks and to address this issue successfully, it must prioritise improving cyber defence capabilities, develop a comprehensive cyber risk mitigation strategy, and promote international cooperation to combat cybercrime's extent. This essay aims to explore and analyse the challenges for cyber defense within the context of the CSDP. The CSDP serves as the cornerstone of the EU's efforts to ensure peace, stability, and security among its Member States. As cyberspace continues to evolve rapidly, it poses threats to critical infrastructure. Sensitive information and national security have also multiplied.<sup>1</sup>

One of the primary challenges the CSDP faces in cyber defence is the rapidly evolving threat landscape. Cyber adversaries are becoming increasingly sophisticated, employing advanced techniques and exploiting vulnerabilities in networks and systems. The emergence of new attack vectors and the evolving nature of cyber threats necessitate adaptive and agile defence measures within the CSDP framework. Staying ahead of these threats requires constant monitoring, analysis, and the development of innovative strategies.<sup>2</sup>

Another significant challenge lies in the lack of standardisation across EU Member States regarding cyber defence capabilities, policies, and practices. The varying approaches

---

1 Cf.: Kasper, A. & Mölder, H. (2020). The EU's common security and defence policy in facing new security challenges and its impact on cyber defence. *The EU in the 21<sup>st</sup> Century: Challenges and Opportunities for the European Integration Process*. Springer International Publishing. P. 271-294.

2 Cf.: Burrell, D.N. (2018). An Exploration of the Cybersecurity Workforce Shortage. *International Journal of Hyperconnectivity and the Internet of Things*. IGI Global. Vol. 2 No. 1. P. 29-41.

make levels of seamless coordination and cooperation among Member States difficult. Standardising cyber defence policies and practices is vital to establish a robust and cohesive defence framework.<sup>3</sup>

Furthermore, the limited information sharing among Member States poses a considerable obstacle to effective cyber defence within the CSDP. However, concerns over national security, data protection, and confidentiality often impede the free flow of information. Building trust, establishing secure communication channels, and facilitating information exchange mechanisms are essential for enhancing collaboration and response capabilities.<sup>4</sup>

Additionally, the field of cyber security is highly specialised and the demand for experts far exceeds the current supply. Addressing this skill gap requires investments in training programmes, education initiatives, and collaborations with academia and industry. By expanding the pool of cyber professionals, the CSDP can enhance its cyber defence capabilities and effectively respond to evolving threats.<sup>5</sup>

---

3 Cf.: Ataç, C. and Akleyek, S. (2019). A Survey on Security Threats and Solutions in the Age of IoT. *European Journal of Science and Technology*. Vol. 15 No. 15. P. 36-42.

4 Cf.: Deloitte Bedrijfsrevisoren, Jo De Muynck and Dr. Silvia Portesi. (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches*.

5 Cf.: Burrell, D.N. (2018). An Exploration of the Cybersecurity Workforce Shortage. *International Journal of Hyperconnectivity and the Internet of Things*. IGI Global. Vol. 2 No. 1. P. 29-41.

## 4. Current State of Research

The current state of research regarding cyber defence in the context of the CSDP reflects the growing recognition of the importance of cyber security within the EU framework. Scholars, policy experts, and practitioners have focused on various aspects of cyber defence to understand the challenges and develop effective strategies. Here is an overview of the key themes and findings based on the existing research:

- **Evolving Cyber Threat Landscape:** Researches highlighted the dynamic and evolving nature of cyber threats faced by the CSDP. Studies have explored different types of cyberattacks, including malware, phishing, ransomware, and state-sponsored cyber espionage. An understanding of the evolving threat landscape is crucial for developing proactive cyber defence measures.<sup>6</sup>
- **Capacity Building and Collaboration:** Scholars emphasised the importance of capacity building and collaboration among EU Member States to enhance cyber defence within the CSDP. Researches highlighted the need to standardise cyber defence policies, information-sharing mechanisms, and joint exercises to build trust and improve coordination. Studies also emphasised the significance of public-private partnerships and collaboration with industry stakeholders to leverage expertise and resources in tackling cyber threats.<sup>7</sup>
- **Legal and Policy Frameworks:** The researchers examined the legal and policy frameworks that govern cyber defence within the CSDP. Scholars explored EU directives and regulations related to data protection, privacy, and information sharing in the context of cyber defence. An understanding of the legal dimensions of cyber defence is crucial for ensuring compliance and effective response.<sup>8</sup>

The current researches on cyber defence within the CSDP provide valuable insights into the evolving threat landscape, the importance of capacity building and collaboration, legal

---

6 Cf.: Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security. Elsevier Advanced Technology*. Vol. 30 No. 8. P. 719-731.

7 Cf.: John Hering, Pablo Hinojosa and Eneken Tikk. (2021). Mapping and Analysis of International Cybersecurity Norms Agreements. *IGF Internet Governance Forum*. P. 13.

8 Cf.: Creese, S., Dutton, W.H., Esteve-González, P. and Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy. Routledge*. Vol. 6 No. 2. P. 214.

considerations, cyber defence capabilities, and information sharing. These findings contribute to a better understanding of the challenges and opportunities for cyber defence in the context of the CSDP.



## 5. Research Gap

Despite the existing body of research on cyber defence in the context of the CSDP, several research gaps still need to be addressed. These research gaps highlight areas where further investigation is required to deepen our understanding and develop more comprehensive strategies for cyber defence within the CSDP.

The lack of clear strategies for standardisation addresses the need for greater harmonisation in cyber defence capabilities, policies, and practices across EU Member States within the CSDP. Further researches are needed to explore and develop practical approaches, guidelines, and frameworks to facilitate the standardisation of cyber defence efforts, promote coordination, and ensure a collective and cohesive response to cyber threats within the CSDP.<sup>9</sup>

The research gap may exist regarding the limited understanding of the specific barriers and challenges that hinder practical information sharing in the context of cyber defence. Further researches are needed to identify and analyse these barriers, such as concerns over national security, legal and policy constraints, technological limitations, and the lack of trust and cooperation. Additionally, exploring potential solutions, such as secure communication channels, information exchange mechanisms, and building trust among Member States, will contribute to bridging this research gap.

---

9 Cf.: Homepage of cyberdefensemagazine.com. URL: <https://cyberdefensemagazine.com/solving-cybersecurity-problems-arising-in-difficult-environments-of-high-uncertainty/>. [9-6-23].

## **6. Research Questions**

The main research question is:

What are the challenges for cyber defence in the context of the Common Security and Defence Policy?

To be able to answer this question, the following issues must be addressed:

- Which are the focal points of the CSDP against cybercrime?
- Which are the cyber threats for CSDP?
- How should the cyber defence capacity be enhanced?

## **7. Methodology**

The research design adopts a mixed-methods approach, combining qualitative and quantitative research methods. The qualitative component involves a thorough literature review, identifying existing researches, scholarly articles, reports, and policy documents related to cyber defence within the CSDP. This literature review serves as the foundation for understanding the current state of knowledge, identifying research gaps, and informing the research process.

The quantitative component involves the analysis of existing data sources, such as publicly available reports and statistical data, to gather objective information and insights into the cyber defence landscape within the CSDP. This quantitative analysis provides a broader perspective and statistical trends related to cyber defence challenges, standardisation efforts, and information-sharing practices. The limitations of the research include the potential lack of coverage of every EU Member State within the CSDP due to resource restrictions. This research provides valuable insights and recommendations for enhancing cyber defence capabilities within the CSDP, addressing the challenges identified.

Already established research methods are followed to ensure the validity and reliability of the research findings. Some ethical guidelines are taken into consideration as well.

## 8. Research and Results of Research

This section presents the results and findings obtained from the research on cyber defence within the CSDP. The findings are discussed in relation to the research questions and provide insights into the challenges and opportunities for cyber defence within the CSDP.

### 8.1 The focal Points of Cyber Defence in CSDP

The CSDP developed gradually between 1999 and 2003 and was expanded by the Lisbon Treaty, which came into force in 2009. CSDP is one of the most important instruments of military and civilian measures to maintain the peace of the EU Member States. The EU is currently conducting six military operations and eleven civil missions. The CSDP is an essential framework for developing EU cyber defence policy and capabilities.<sup>10</sup>

Following the aggressive increase of cyberattacks with devastating economic damages and the Russian invasion of Ukraine, the EU has adopted a new action plan to enhance its ability to prevent, detect, deter, and defend. It is built around four pillars:

Pillar 1: Act together for a stronger EU cyber defence

The EU wants to improve coordination within national cyber actors, strengthen cooperation between military and civilian cyber communities, and support the CSDP military operations and civilian missions. Therefore, it is essential to establish an EUCDCC (EU Cyber Defence Coordination Centre), including all EU military CSDP commanders.<sup>11</sup>

Pillar 2: Secure the EU defence ecosystem

This includes the development of legally binding recommendations for the EU on cyber defence, the elaboration of critical infrastructure risk scenarios for the military, and

---

10 Cf.: Homepage of the Federal Ministry Republic of Austria. URL: <https://www.bmeia.gv.at/en/European-foreign-policy/security-policy/common-european-security-and-defence-policy-csdp/>. [8-6-23].

11 Cf.: Homepage of the European Union. URL: <https://www.eeas.europa.eu/sites/default/files/documents/Factsheet%20-%20The%20EU%20policy%20on%20cyber%20defence.pdf>. [8-6-23].

measures to improve cooperation in developing standards and certifications for dual-use products.<sup>12</sup>

Pillar 3: Investing in our cyber defence capabilities

Developing a technology roadmap for critical cyber technologies, investing in modern military cyber defence capabilities, and establishing an EU Cyber Skills Academy are critical issues for this pillar.<sup>13</sup>

Pillar 4: Partnering to address common challenges

The focus of this pillar is strengthening the EU-NATO cooperation in cyber defence training, strengthening existing partnerships, and establishing new partnerships in the field of cyber defence.<sup>14</sup>

## **8.2 The Cyber Threats for CSDP**

Cyberattacks consist of criminal acts committed online using electronic communication networks and information systems. Cyberattacks are attempts to misuse information by stealing, destroying, or disclosing it. Cybercrimes are frequently conducted today and the main goal shifted from harming single targets in financial aspects to attacking industrial organisations, critical infrastructure, or state alliances.

The infographic released by the ENISA (European Union Agency for Cybersecurity), published on 11 11 2022, describes the top ten cybersecurity threats at the present and for the future.

---

12 Cf.: *ibid.*

13 Cf.: *ibid.*

14 Cf.: *ibid.*



**Figure 1:** Cyber threats.<sup>15</sup>

The generic terms for the varieties of attacks are mentioned above in figure 1. Since describing all of them and their sub-terms in detail would go beyond the scope, there are a few new trends in cyberattacks highlighted by the author. According to the latest ENISA studies, the operational technology will increasingly become a high-value target for threat actors. It must be mentioned that those actors' current intent is not disruption. Instead, their main goal is targeting systems to gather information. The purpose of this is that exploiting those systems gives them multiple targets they can take advantage of.

On the other hand, as seen in the Russian-Ukraine war, cyberattacks are constantly joined with military operations. For instance, the infamous wiper attacks can shut down the network between governmental agencies and critical infrastructure. The aim of such attacks is to pave the way for disinformation operations to unsettle the people's trust in the government.<sup>16</sup> The threat actors are considered hacktivists, state-sponsored hackers,

<sup>15</sup> Homepage of the European Union Agency for Cybersecurity. URL: [file:///C:/Users/krist/Downloads/ENISA%20Threat%20Landscape%202022%20\(1\).pdf](file:///C:/Users/krist/Downloads/ENISA%20Threat%20Landscape%202022%20(1).pdf). [8-6-23].

<sup>16</sup> Cf.: Ifigeneia Lella, Eleni Tsekmezoglou, Rossen Svetozarov Naydenov, Cosmin Ciobanu, Apostolos Malatras, Marianthi Theocharidou. (2022). ENISA Threat Landscape 2022. ENISA (European Union Agency for Cybersecurity). P. 24.

hacker-for-hire actors, and cybercrime actors.<sup>17</sup> The hacker-for-hire trend is nothing new. There have always been companies that provided their customers with offensive software or hardware, primarily for governments. On the other hand, hacktivism is a relatively new term and went viral through the call of Ukraine's deputy prime and digital transformation minister for volunteers to go after specific targets coordinated through the Telegram app.<sup>18</sup>

However, not only during the Russian-Ukraine such attacks took place, but also towards the government of Mozambique, which attack shut down their websites.<sup>19</sup>

Cyberattacks in the form of politically-themed phishing emails and decoy documents harmed Palestinian activists.<sup>20</sup>

In Libya, the check point research discovered that high-value targets were attacked with cyber espionage through malware. Also, phishing domains were disguised as websites of the Ministry of Foreign Affairs.<sup>21</sup> These are just a few examples of countries where an ongoing CSDP mission or operation takes place.

The most common malware attacks range from denial-of-service attacks, phishing, and ransomware attacks to cyber espionage. The latest and most dangerous tool that hackers use is artificial intelligence. With this tool, the user is able to automate attacks, which are constantly adapting and developing themselves to gain access to systems.<sup>22</sup>

---

17 Cf.: *ibid.* P. 22.

18 Cf.: *ibid.* P. 28.

19 Cf.: Homepage of GlobalVoices.org. URL: <https://globalvoices.org/2022/03/02/mozambican-government-websites-suffer-cyber-attack/>. [9-6-23].

20 Cf.: Homepage of thehackernews.com URL: <https://thehackernews.com/2022/02/new-wave-of-cyber-attacks-target.html>. [9-6-23].

21 Cf.: Homepage of hackread.com. URL: <https://www.hackread.com/espionage-malware-stealth-soldier-libya/>. [9-6-23].

22 Cf.: Homepage of it-day.net. URL: <https://www.it-daily.net/it-sicherheit/cybercrime/ki-gegen-ki-das-wetruersten-in-der-cyber-abwehr-geht-weiter>. [7-6-23].

### **8.3 The Enhancement of Cyber Defence**

Under the CSDP, building cyber defence capabilities necessitates an all-encompassing strategy. It contains the creation of strategies, competencies, frameworks for the law, awareness, and collaboration between the public and private sectors. The CSDP also needs to foster a sense of mutual respect and acceptance that cybersecurity is a shared responsibility.

International collaboration and synergies are required to boost reciprocal capacity building in order to accomplish this. Additionally, the development of cyber defensive capabilities requires the purchase of new technologies, standards, strategies, and training. The members of the CSDP ought to encourage the sharing of knowledge and resources in order to improve their capacity for collaboration with other private actors. The CSDP is to be strengthened by enhancing knowledge, production, awareness, and other cyber defence capabilities through technology and collaboration.

The CSDP can be better prepared to achieve its goals, deal with any obstacles, and strengthen its ability to defend itself against cyberattacks by taking a comprehensive approach to capacity building. Most of the EU Member States either have or are creating national cybersecurity strategies. However, these techniques' goals and the development of cybersecurity vary from nation to nation. Determining if these measures are in line with the CSDP's goals and coordinating efforts to improve the EU's cyber defence capabilities are therefore crucial.

A thorough CSS (Cyber Security Strategy) can offer strategic guidelines to lower cyber defence risks. The EU can adopt a more coordinated and comprehensive strategy to enhance its cyber defence capabilities by integrating state cyber security agendas within the frame of the CSDP.<sup>23</sup> The enhancement of cyber security measures is the key to successful civil missions or military operations in CSDP. It is necessary to set up a secure information and communication central agency in order to keep track of all the data traffic because of all the sensitive information that is circling through the operational area.

---

23 Ibid. P. 21.



For these missions and operations, it is most important to have safe technologies, which are at a state-of-the-art level, for instance, the AI technology, as mentioned above.<sup>24</sup>

### **8.3.1 Cooperation and Information Sharing among Member States**

Not only high-end technology and top-trained employees are enough to take cyber defence to the next level. Without tight cooperation between partners – external as well as internal – and institutions, a major aspect of cyber defence is missing. Exercises help states to get a better understanding of how their processes in cyber defence work and how they are set up in case of incidents. This information exchange between military and civilian partners is very beneficial for CSDP missions and operations to be successful throughout the timespan of an active one. Merging the civilian and military knowledge and measures will be the key to having a permanently high level of cyber defence capabilities. Sharing information and working together to solve problems are two of the most important components of an effective capacity-building programme. Because trust is a process but not a state regular action needs to be taken to build it. A lack of trust among members can lead to an inability to share information about security incidents, which can affect an organisation's ability to improve its cyber security. Public-private partnerships have the potential to play a key role in building higher levels of trust. According to the ISF (Information Sharing Framework) developed by the MACSSA 2013 (Multinational Alliance for Collaborative Cyber Situational Awareness), information sharing is based on authentication, authorisation, and accountability. To effectively combat cyber threats, The EU Member States must work together to build a culture of trust and information sharing.<sup>25</sup>

### **8.3.2 Investment in Cyber Defence Technologies and Training**

According to the study by the European Investment Bank, an amount of 7.5 billion euros will be allocated over the years 2021 to 2027 to meet the high demands of the AI sector,

---

24 Cf.: Homepage of the European Union of External Action. URL: [https://www.eeas.europa.eu/sites/default/files/documents/Comm\\_cyber%20defence.pdf](https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf). [30-5-23].

25 Cf: Trimintzios, P. & Security, E. U. A. F. N. A. I. (2017). Cybersecurity in the EU CSDP (Common Security and Defence Policy): Challenges and Risks for the EU: Study. P. 26.

supercomputing, and cybersecurity, and 1.6 billion euros will be allocated to EU cyber defence.<sup>26</sup> In direct comparison, out of 40 companies worldwide that generate more than 1 billion in revenue per year with AI-based systems, China generates 15 ones and the USA 20 ones.<sup>27</sup> The most important aspect of cyber defence capabilities is the persons who work with ICT devices. To use these devices safely, it is vital to be constantly trained and kept up to date because the technologies rapidly change, adapt, and evolve quickly. Therefore, it is necessary to get specialists to train users of ICT devices and help developing a very good understanding of what threats could look like and the correct way to behave when an incident happens. To achieve this effect, it is necessary to set high standards and requirements for specialists and for cyber advisers because they have to understand the legal terms and the military aspect of being able to make valuable decisions if an incident occurs. To educate these specialists further, there have to be frequent exercises for reducing the mind gap between the decision-makers and the advisers.<sup>28</sup>

In addition, private enterprises offer a lot of the essential services that society depends on and they ought to be involved in the conversation about how to safeguard these services from cybercrime.

To stop the spread of cyberattacks, data communications are equally critical. To lessen the effects of assaults, the private sector must cooperate with and exchange information with the institutions targeted. To protect users, software developers might exchange details about recent or rumoured threats. This collaboration should continue until hazards are successfully reduced. The EU Member States can more effectively defend the digital economy from cyber-attacks by investing in cybersecurity technologies, training, and collaboration with the private sector.<sup>29</sup>

---

26 Cf.: Brendan McDonagh, Carlos Munoz, Maria Lundqvist, Ioannis Bouzopoulos and Pierre-Alain Francois. (2022). European Cybersecurity Investment Platform. European Investment Bank. P. 41.

27 Cf.: Homepage of moderndiplomacy.eu. URL: <https://moderndiplomacy.eu/2023/05/23/u-s-china-and-russia-intelligence-cybersecurity-and-new-developing-technologies/>. [3-6-23].

28 Cf.: Amorim, L., Biscop, S. & Dubois, D. (2021). Handbook on CSDP 4<sup>th</sup> edition. Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria. P. 128. [30-5-23].

29 Cf.: Trimintzios, P. & Security, E. U. A. F. N. A. I. (2017). Cybersecurity in the EU CSDP (Common Security and Defence Policy): Challenges and Risks for the EU: Study. P. 24-28.

## 9. Discussion of Results and personal Conclusions

According to the global rise in cybercrime, which not only causes significant damage to the economy but also threatens the foundations of a state and the basic functioning of society, the EU did react. New laws and regulations were passed in November 2022, such as the Network and Information Security Directive, which tightened cybersecurity requirements for medium and large companies in key sectors and extended their scope to other sectors, including energy, transport, banking, health, digital infrastructure, public administration, and space. The DORA (Digital Operational Resilience Act), a regulation on the operational stability of digital systems of the financial sector, was adopted to protect the financial sector, and regulations were issued to improve the protection of critical infrastructure as well. It shows the acute need for action and the complex and diverse challenges, which the CSDP has to face.<sup>30</sup>

Firstly, the rapidly evolving threat landscape demands agile defence measures, continuous monitoring, and innovative strategies to prevent potential attacks. Secondly, the lack of standardisation in cyber defence capabilities, policies, and practices across EU Member States obstructs effective coordination. Standardisation and certification policies and practices promote information sharing and efficient resource allocation for a robust response. Thirdly, limited information sharing hinders proactive cyber defence in the CSDP, necessitating secure and timely information exchange mechanisms for collaboration and swift response. Finally, the shortage of skilled cyber defence professionals requires investments in training, education, and intensive collaborations with industry and academia.

The cybersecurity threats are constantly changing and can originate from many different places, creating significant challenges for organisations in their efforts to protect themselves online. To address these challenges, the European Union needs to adopt a comprehensive and coordinated approach to cyber defence. This approach requires the adoption of common cybersecurity standards and legislation, the sharing of best practices

---

30 Cf.: Homepage of Aktuelles Europäisches Parlament. URL: [---

Page 17 of 23](https://www.europarl.europa.eu/news/de/headlines/security/20221103STO48002/neue-gesetze-im-kampf-gegen-cyberkriminalitat#:~:text=Schutz%20des%20Finanzsystems%20der%20EU%20%E2%80%93%20DORA&text=November%202022%20endg%C3%BCltig%20verabschiedet.,der%20EU%20eingef%C3%BChrt%20und%20harmonisiert. [10-6-23].</a></p></div><div data-bbox=)

and experiences, and closer cooperation with international organisations and private sector actors. The development of CSDP cyber defence capabilities requires policies, strategies, skills, legal frameworks, awareness, and understanding in both the public and private sectors. The EU also needs standardised procedures in case of cyber incidents and not only is it well required, but there is also an urgent need to set software and hardware standards for the Member States to ensure that attackers do not get access to the EU cyberspace because members do not follow the same requirements and some of them have a weaker cyber defence system than the other ones.

It is important to promote collaboration. Monitoring all the conducted cyberattacks is a brilliant method to keep up with the cyber threat actors. In the long run, states will be able to track the trends of attacks and in which directions the new trends will lead. The exchange of knowledge and tools, as well as the acquisition of new technologies, standards, regulations, and training, are all necessary for developing cyber defensive capabilities.

Additionally, by connecting national cybersecurity plans to CSDP goals, it is possible to give the strategic principles and direction required to reduce cybersecurity risks and effectively address new cyber threats. In addition, linking national cybersecurity plans to CSDP objectives can provide the strategic principles and guidance needed to mitigate cybersecurity risks and respond effectively to emerging cyber threats. This can be achieved by aligning national cybersecurity strategies with the objectives of the CSDP.

The challenges of the CSDP in cyber defence require a coordinated and comprehensive approach that should include cooperation with various stakeholders at national and international levels. This will enable the CSDP to effectively mitigate cybersecurity risks and threats, thus ensuring the security of the EU and its citizens in the digital age. Building a cyber competence, which develops comprehensive defence and attack software fit for the future is imperative. Investing in cyber defence means investing in the future.

## 10. Annexes

### 10.1 List of Abbreviations

AI .....	Artificial Intelligence
CSDP .....	Common Security and Defence Policy
CSS .....	Cyber Security Strategy
DORA .....	Digital Operational Resilience Act
ENISA .....	European Union Agency for Cybersecurity
EU .....	European Union
EU MS .....	European Union Member State
EUCDCC .....	European Union Cyber Defence Coordination Centre
ICT .....	Information and Communication Technology
ISF .....	Information Sharing Framework
IT .....	Information Technology
MACSSA .....	Multinational Alliance for Collaborative Cyber Awareness
NATO .....	North Atlantic Treaty Organization
NIS .....	Network and Information Security

**10.2 List of Figures**

<b>No.</b>	<b>Figures' Descriptions</b>	<b>Page</b>
1	Cyber threats.	12

## 10.3 List of Literature

### 10.3.1 Books

- 01 Ataç, C. and Akleylek, S. (2019). A Survey on Security Threats and Solutions in the Age of IoT. *European Journal of Science and Technology*. Vol. 15 No. 15.
- 02 Bendovschi, A. (2015). *Cyber-Attacks - Trends, Patterns and Security Countermeasures*. *Procedia Economics and Finance*. Elsevier. Vol. 28.
- 03 Brendan McDonagh, Carlos Munoz, Maria Lundqvist, Ioannis Bouzopoulos and Pierre-Alain Francois. (2022). *European Cybersecurity Investment Platform*. European Investment Bank. <https://doi.org/10.2867/943253>.
- 04 Brilingaite, A., Bukauskas, L., Juozapavičius, A. and Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity*. Oxford Academic, Vol. 8 No. 1.
- 05 Burrell, D.N. (2018). An Exploration of the Cybersecurity Workforce Shortage. *International Journal of Hyperconnectivity and the Internet of Things*. IGI Global. Vol. 2 No. 1.
- 06 Choo, K.K.R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*. Elsevier Advanced Technology. Vol. 30 No. 8.
- 07 Creese, S., Dutton, W.H., Esteve-González, P. and Shillair, R. (2021). Cybersecurity capacity-building: cross-national benefits and international divides. *Journal of Cyber Policy*. Routledge. Vol. 6 No. 2.
- 08 Deloitte Bedrijfsrevisoren, Jo De Muynck and Dr. Silvia Portesi. (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-Regulatory Approaches*.
- 09 Ifigeneia Lella, Eleni Tsekmezoglou, Rossen Svetozarov Naydenov, Cosmin Ciobanu, Apostolos Malatras, Marianthi Theocharidou. (2022). *ENISA Threat Landscape 2022*. (ENISA) European Union Agency for Cybersecurity.
- 10 John Hering, Pablo Hinojosa and Eneken Tikk. (2021). *Mapping and Analysis of International Cybersecurity Norms Agreements*. IGF Internet Governance Forum.
- 11 Kasper, A. and Mölder, H. (2020). *The EU's common security and defence policy in facing new security challenges and its impact on cyber defence*. *The EU in the 21st Century: Challenges and Opportunities for the European Integration Process*. Springer International Publishing.
- 12 Liaropoulos, A. N. and Giasas, D. (2019). *Cybersecurity in the EU: Threats, Frameworks and future perspectives*. *Cybersecurity in the EU: Threats, Frameworks and Future Perspectives*.
- 13 Trimintzios, P. & Security, E. U. A. F. N. A. I. (2017). *Cybersecurity in the EU (CSDP) Common Security and Defence Policy: Challenges and Risks for the EU: Study*.

### 10.3.2 Internet

- 01 Homepage of GlobalVoices.org. URL: <https://globalvoices.org/2022/03/02/mozambican-government-websites-suffer-cyber-attack/>. [9-6-23].
- 02 Homepage of hackread.com. URL: <https://www.hackread.com/espionage-malware-stealth-soldier-libya/>. [9-6-23].
- 03 Homepage of it-day.net. URL: <https://www.it-daily.net/it-sicherheit/cybercrime/ki-gegen-ki-das-wettruesten-in-der-cyber-abwehr-geht-weiter/>. [7-6-23].
- 04 Homepage of moderdiplomacy.eu. URL: <https://moderndiplomacy.eu/2023/05/23/u-s-china-and-russia-intelligence-cybersecurity-and-new-developing-technologies/> [3-6-23].
- 05 Homepage of the European Union Agency for Cybersecurity. URL: [file:///C:/Users/krist/Downloads/ENISA%20Threat%20Landscape%202022%20\(1\).pdf](file:///C:/Users/krist/Downloads/ENISA%20Threat%20Landscape%202022%20(1).pdf). [8-6-23].
- 06 Homepage of the European Union Agency for Cybersecurity. URL: [file:///C:/Users/krist/Downloads/ENISA%20Threat%20Landscape%202022%20\(1\).pdf](file:///C:/Users/krist/Downloads/ENISA%20Threat%20Landscape%202022%20(1).pdf). [8-6-23].
- 07 Homepage of the European Union of External Action. URL: [https://www.eeas.europa.eu/sites/default/files/documents/Comm\\_cyber%20defence.pdf](https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf). [30-5-23].
- 08 Homepage of the European Union. URL: <https://www.eeas.europa.eu/sites/default/files/documents/Factsheet%20-%20The%20EU%20policy%20on%20cyber%20defence.pdf>. [8-6-23].
- 09 Homepage of the Federal Ministry Republic of Austria. URL: <https://www.bmeia.gv.at/en/european-foreign-policy/security-policy/common-european-security-and-defence-policy-csdp/>. [8-6-23].
- 10 Homepage of thehackernews.com. URL: <https://thehackernews.com/2022/02/new-wave-of-cyber-attacks-target.html>. [9-6-23].
- 11 Homepage of cyberdefensemagazine.com. URL: <https://www.cyberdefensemagazine.com/solving-cybersecurity-problems-arising-in-difficult-environments-of-high-uncertainty/>. [9-6-23].

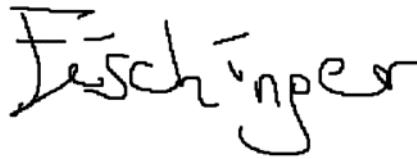


## 11. Affidavit

I declare that I have written the present essay independently and on my own. I have clearly marked any language or ideas borrowed from other sources as not my own and documented their sources. The essay does not contain any work that I have handed in or have had graded as a previous scientific paper earlier on.

I am aware that any failure to do so constitutes plagiarism. Plagiarism is the presentation of another person's thoughts or words as if they were my own – even if I summarise, paraphrase, condense, cut, rearrange, or otherwise alter them.

I am aware of the consequences and sanctions plagiarism entails. Among others, consequences may include nullification of the essay and exclusion from participation in the CSDP Olympiad. These consequences also apply retrospectively, i.e., if plagiarism is discovered after the essay has been accepted and graded. I am fully aware of the scope of these consequences.



.....

(Kristof Fischinger)

Wiener Neustadt, Austria in October 2023