Leiden University

What is the added value of the EU membership in the field of cybersecurity?

Master Thesis

Name:	Matyas Safranka
Student number:	2571544
Student email:	m.safranka@umail.leidenuniv.nl
Study:	European Union Studies Master
Supervisor:	Dr Maxine David
Submission date:	24/06/2021
Word count (excluding bibliography):	14489

What is the added value of the EU membership in the field of cybersecurity?

Matyas Safranka (2571544)

Leiden University

Master thesis

What is the added value of the EU membership in the field of cybersecurity?

This page was intentionally left empty.

The author of this paper is an employee of Microsoft corporation. The views and thoughts presented in this paper are his own and do not represent the official views of Microsoft corporation.

Table of Contents

What is the added value of the EU membership in the field of cybersecurity?

Verklaring van originaliteit / Declaration of originality

By submitting this thesis, I certify that:

- ✓ this work has been drafted by me without any assistance from others
- ✓ I have not discussed, shared, or copied assessment work from/with other students;
- ✓ I have not used sources that are not explicitly allowed by the course instructors and I have clearly referenced all sources (either from a printed source, internet or any other source) used in the work in accordance with the course requirements and the indications of the course instructors;
- ✓ this work has not been previously used for other courses in the program, unless explicitly allowed by the instructors.

I understand that any false claim in respect of this work will result in disciplinary action in accordance with university regulations and the program regulations, and that any false claim will be reported to the Board of Examiners. Disciplinary measures can result in exclusion from the course and/or the program, and in a permanent endorsement on my diploma.

I understand that my work may be checked for plagiarism, by the use of plagiarism detection software as well as through other measures taken by the university to prevent and check on fraud and plagiarism.

I understand and endorse the significance of the prevention of fraud and I acknowledge that in case of (gross) fraud the program could declare the exam invalid, which may have consequences for all students.

Abbreviations

BEREC	Body of European Regulators for Electronic Communication
CCDCOE	Cooperative Cyber Defence Centre of Excellence (NATO)
CERT	Computer Emergency Response Teams
CFSP	Common Foreign and Security Policy
CSIRT	Computer Security Incident Response Teams
CoE	Council of Europe
COREPER	Committee of the Permanent Representatives of the Governments of the Member States to the European Union
CSDP	Common Security and Defence Policy
EEAS	European External Action Service
ENISA	European Union Agency for Cybersecurity
ESDC	European Security and Defence College
ICT	Info Communication Technology
JHA	Justice and Home Affairs
NATO	North Atlantic Treaty Organisation
NIS Directive	Directive 2016/1148 on the security of network and information systems
OSCE	Organization for Security and Co-operation in Europe
PESCO	Permanent Structured Cooperation
PSC	Political and Security Committee (within the COREPER)
UN	United Nations

What is the added value of the EU membership in the field of cybersecurity?

Abstract

This research aims to contribute to the debates on the democratic deficit of the European Union by researching the added value of EU membership in the field of cybersecurity. One of the main arguments when discussing the democratic deficit of the EU, argues that the EU fulfils its democratic purposes, if it works 'for' the people. By providing effective governance and polity, the EU membership makes cyberspace safer and more secure for its member states, which is beneficial for all EU citizens. The EU and its agencies facilitate effective and operative cooperation that works 'for' the people. This research focused on two member states as case studies, The Netherlands and Hungary and found evidence that the EU provides a trusted and operative environment which contributes to cybersecurity in unique ways like no other international cooperation. This research looks for evidence that Europeanization, securitization, and interdependence drive the integration in cybersecurity at the European level.

Keywords: EU, European Union, cybersecurity, securitization, Europeanization, democratic deficit, Hungary, Netherlands

Introduction

In the last 30 years, information communication technologies (ICT) have drastically changed our society. The internet in the 1980s was an interconnection of university and research institutions' local networks to provide faster collaboration and information access for researchers. The access was limited to a small group of researchers. What once was the interests only of academics, technology enthusiasts, and later businesses is now an integral part of our everyday lives. Online connected smart devices are not only enabling communication with friends and relatives, faster shopping or an option for online administration, but these technologies are now integral parts of everyday life. Leveraging new technologies such as Internet-of-Things (IoT), Artificial Intelligence (AI), and 5G will further accelerate this dependency on technology. This dependency introduced new threats as well. Examples of the most recent cybersecurity attacks in the EU were: "European Medicines Agency was breached; cyber espionage campaigns targeted several government officials including Belgium's interior minister and dozens of Polish politicians; and hospitals in Ireland and France have sustained ransomware attacks" (Laurens Cerulus 2021). Ransomware attacks on hospitals can even threaten human life (Lee Mathews 2020). The digital transformation of societies also meant that most threats to national safety and security transitioned to cyber.

Recent developments in cyberattacks made governments realize that cyberspace means new threats due to its unique characteristics. These include the cross-border nature, which allows attackers from anywhere in the world to conduct attacks. Due to the connected nature of modern infrastructure, there can be collateral damage outside the target. If an attacker releases malware – a malicious software code – it attacks every vulnerable system available online. The anonymous nature of the online world makes the collection of evidence and attribution a lot more difficult, if not impossible. The malicious actors can be criminals, nation-states, or both; the events in cyberspace can "spill over into physical terrorism" (Gabi Siboni and David Siman-Tov 2014). A large amount of data and information shared online makes identifying malevolent intentions in time also challenging for the authorities. Misinformation and disinformation enhanced by social networks influence outcomes of elections (Lisa-Maria Neudert, Philip Howard, and Bence Kollanyi 2019) and cyberattacks are debated in election campaigns (Alicia Parlapiano 2016).

What is the added value of the EU membership in the field of cybersecurity?

One of the core tasks of every state is to provide safety and security to its citizens. In its current form, the European Union is not a state but a unique polity and governance entity that directly impacts its citizens' lives. Though it was originally intended to guarantee peace on the continent, the EU is neither a security nor a defence organization, unlike NATO. This research aims to investigate the added value of the EU in the field of cybersecurity to the member states and citizens. This thesis hypothesises that through Europeanization, securitization, and interdependence, the EU contributes to the security of cyberspace for the member states and citizens. This research aims to investigate two selected EU and NATO member states - The Netherlands and Hungary - as case studies to identify the unique added values of the EU membership in the field of cybersecurity. The research does not intend to identify generic values in international cooperation in the field of cybersecurity; it explicitly focuses on unique values provided by the EU. This research argues that by facilitating effective governance and unique values in cybersecurity, the EU fulfils its democratic role by working for its citizens' safety, security, and common interests.

The research first reviews the literature on the relevant theories, including the debates on the democratic deficit of the EU, Europeanization, securitization, and interdependence in a cybersecurity context. The literature review also introduces relevant concepts and aspects of cybersecurity that used in the analysis. The methodologies chapter describes the methods used in the analysis. The findings are arranged by country and, per unit of analysis, government documents. The discussion chapter then summarizes the findings of the analysis in the context of the original hypothesis and literature. The conclusion chapter drives the general conclusions and findings and identifies the additional areas for further research.

Literature review

This chapter provides the overview of relevant literature required to answer the research question: what the added value of EU membership in the field of cybersecurity is. First, this chapter provides an overview of relevant European Union studies literature, as this research aims to contribute to the discussion on the democratic deficit of the EU. This first part focuses on the debates on the democratic deficit of the EU, Europeanization, politicization, and securitization of cybersecurity. The second part of the literature review focuses on cybersecurity discussions and cooperation of states in the field, intending to provide the necessary context for the analysis.

If we rephrase this research question, this research aims to find answers to how EU membership contributes to the security and well-being of the citizens of the member states in cyber-space. It is relevant to understand the EU's value to its citizens as an effective polity entity because this is one of the arguments in the debates on the democratic deficit of the EU. One aspect of the debate on the EU's democratic deficit organized around the question of democracy 'of' and 'by' the people (Zimmermann and Dür 2016, 64–79). Weiler and Hix argue that a pan-European 'demos' would be required to eliminate the democratic deficit of the European Union as democratic governance of the people can only be achieved if there is a pan-European demos, as only such can give democratic authorization to the institutions (Weiler 1995) (Simon Hix 2008). However, Moravcsik, Majone and Scharpf introduced another argument in the debate on the EU's democratic deficit: democracy 'for' the people (Majone 1998; Moravcsik 2002; Scharpf 1999). They argue that decisions decided by majorities not necessary always serve the general public interest. They argue that governance 'by' the people is relevant for redistributive policies, while for regulatory policies, the 'for' the people aspect is more critical as regulatory policies not necessary most effective if those are decided 'by' majority of the people. As Richard Bellamy argues, sometimes it is essential to "depoliticize certain key policy areas [and], limiting 'input' democracy 'by' the people so as to provide a more effective democratic 'output' that delivers rule 'for' the people" (Zimmermann and Dür 2016, 70). In other words, the EU fulfils its democratic purpose if it facilities an environment that provides governance and polity that serves the `generic interests of the people, better than what the member states individually could. Therefore, this thesis investigates if there is evidence that the EU provides such benefits and therefore contributes to a more secure cyber-space for the citizens. It is also important to investigate whether the EU is

efficient when fulfilling these goals. Mats Peterson argues that the EU is efficient in adopting new rules and regulations, but it is not efficient to "adapt to the economic and political challenges of the modern, globalized world" (Zimmermann and Dür 2016, 38). Majone also argues that "the Monnet method turned out to be flawed since its votaries never resolved a crucial dilemma: whether European policies should be initiated in order to solve specific problems in the best possible way, or whether they are to serve, first and foremost, integration objectives" (Majone 2005, vii). In other words, Majone argues that integration most likely results in suboptimal results.

Carrapico and Barrinha concluded that the EU is gradually becoming an important actor in the field of cybersecurity as a result of improvement in both horizontal and vertical relations. However, they warn that not all normative assumptions are self-evident, such as EU as a unitary actor is not necessary more effective, or that a more effective EU would be desired as the results of an EU cybersecurity strategy can not only be measured in effectiveness, as it must be also democratic (Carrapico and Barrinha 2017). When Christou investigate the cybercrime governance in the EU through the Joint Cybercrime Action Taskforce (J-CAT) of Europol, he also concludes that there must be a "right balance between security, speed and efficiency and civil liberties in terms of the right to privacy, data protection and free speech" (Christou 2018, 370). Christou also argues that J-CAT is successful because its informal and networked organization nature contributes to effective collaboration (Christou 2018). Odermatt argues that the Network and Information Security Directive (NIS Directive) and advancements in fighting cybercrime legislation eventually replaced soft law. However, he still argues that there is room for further improving collaboration efficiency in cybersecurity (Odermatt 2018).

This research uses the lens of politicization, interdependence and Europeanization in the analysis to find evidence that the EU membership helps improving the security of the cyber-space and, therefore, it contributes to the safety of the citizens. When investigating the European integration through cybersecurity, Fuchs concludes that politicization and interdependence are the main factors (Fuchs 2018). Samonek investigates the three principles of European cooperation (effectiveness, non-aggression and the priority of the European Single Market) in the context of cybersecurity. She concludes that developments in cybersecurity in "the EU is consistent with the trend of Europeanization of wider security policy" (Samonek 2020, 56). She argues that building a resilient cybersecurity system is more effective at an EU level than if member states attempt to secure cyber-space individually. She argues "that the EU member states should pursue a joint

strategy of cybersecurity and cyber defense [sic]" (Samonek 2020, 57). Olsen argues that Europeanization is "an attention-directing device and a starting point for further exploration" (Olsen 2002, 943). Flockhart Cini and Bourne define Europeanization as it "consists of shared beliefs and norms that are first defined and consolidated in the EU policy process and then incorporated in the logic of domestic (national and subnational) discourse, political structures and public policies" (Cini and Bourne 2006, 59). According to Sliwinski, member states will dominate the future of cybersecurity in the EU (Sliwinski 2014) and does not expect any added value from the EU.

EU membership can also improve the state of cybersecurity in member states by providing salience through the securitization of the cyber topic. Securitization of a topic is when a military, political, economic or environmental danger or threat gets into a political discussion, justifying "all available means to counter it" (Tikk and Kerttunen 2020, 11). Tikk and Kerttunen conclude that cybersecurity is securitized in many countries (Tikk and Kerttunen 2020, 18). Christou finds that collective securitization - because of multiple events and threat narratives - played a role in enabling the EU to carry out a cybersecurity policy (Christou 2019). In her 2014 paper, Pernik compares the cybersecurity approach of NATO and the EU. She concludes that both organizations made progress in taking a comprehensive approach to cybersecurity; however, NATO has been more successful. According to Pernik, it is because NATO is mainly a defence focused organization. She also argues that the EU has the potential to become relevant, especially in the other areas of cybersecurity such as "cyber diplomacy, economy or internal security aspects" (Piret Pernik 2014, 15–16). When discussing policing, securitization and democratization in Europe, Loader argues that "threats in fact represent but one of the motors driving the development of European policing" (Loader 2002, 146) and argues that the European project originally was a security project, therefore 'anti-political' acts to preserve 'peace' and 'order' and in general securitization of topics is not alien from the European cooperation (Loader 2002, 147).

Securitization of cybersecurity does not mean that this topic becomes the subset of national security and defence. The review of the relevant literature reveals debates that argue that cybersecurity is distinct from other security despite what the name implies. Boeke et al. investigate what role militaries play in cybersecurity tasks in nations in Asia and Europe. They conclude that though states have different approaches in defence of critical infrastructures, in all cases, militaries have a limited role - if any - when it comes to cybersecurity (Boeke, Heinl, and Veenendaal 2015).

These findings show that cybersecurity as an area does not primarily fall under defence administration. According to Elkhannoubi and Belaissaoui, cybersecurity is a matter of legal, organizational, and technological cooperation between the private sector and national administrations (Elkhannoubi and Belaissaoui 2015). Odermatt explains cybersecurity as an area that overlaps and affects multiple policy areas: Cybersecurity is "blurring of boundaries: between public authorities and non-state actors; between criminal behaviour and politically motivated attacks; between law enforcement and military action; between domestic and international action; between the physical and the online worlds" (Odermatt 2018, 372). Therefore, traditional security and defence cooperation between states (such as NATO, CSDP, PESCO) is not necessarily adequate when investigating cooperation in the field of cybersecurity. Tomic et al. use qualitative analysis to investigate cybersecurity policies in east European EU and non-EU countries. They conclude that "Cybersecurity differs by how countries (1) define a referent object (what should be protected), (2) perceive primary threats and risks, and (3) identify the sources of threats and risks" (Tomic, Saljic, and Cupic 2018, 1054). They setup two categories of states: those who militarize cyberspace and those who refer to criminalization of cyberspace. Cybersecurity has internal affairs aspects such as public safety, policing, counterterrorism, external affairs aspects such as diplomacy and espionage or state defence aspects as well. Investigating it only from one of these aspects would result in leaving relevant aspects of cybersecurity out from this research.

The unit of analysis in this research aims to include all relevant aspects of cybersecurity, which requires defining the term. Di Caillo and Miranda found that there was no common definition of cybersecurity in the EU context, and they use the term cybersecurity as an umbrella that covers cybercrime, cyberattacks, critical infrastructure protection, and regulations on electronic communications (Di Camillo and Miranda 2011). Couzigou also lists cybercrime, cyber espionage, cyberattack, but also potential human errors and accidents that may have harmful impacts on others as areas that need attention when discussing cybersecurity (Couzigou 2018). Christou also identifies that there is no commonly agreed definition of cybersecurity and argues that, though definitions are important, terms can be defined as part of the analysis (Christou 2016). This lack of common taxonomy and definitions makes it challenging to identify terms and compare national policies or define international cooperation (Odermatt 2018, 356). This paper follows the recommendations of Christou and defines terms through the analysis as needed. As a starting point, this research uses the umbrella approach of Couzigou, and Di Caillo and Miranda for

cybersecurity: any area where individual citizens, industry or national interests can be in danger and need protection from a threat that originates from the online space.

The question around state sovereignty is relevant both in the context of the EU and cybersecurity. In the context of the EU, it is relevant as states pool aspects of their sovereignty in the EU. Magnette argues that the classic seventeenth-century thinking on state sovereignty should be replaced with a multi-level governance concept in case of the EU (Magnette 2005, 190). Cyberspace by nature is cross-border and displaces the relevance of state boundaries; boundaries and physical territories do not mean any limit in cyberspace. Therefore, state sovereignty should not only be redefined for an EU context but it should also be investigated what does a state's sovereignty mean in cyberspace. In his article Jensen investigates how state sovereignty works or should work in the field of cybersecurity (Jensen 2015). He argues that although there is no universal definition for state sovereignty in the case of cybersecurity, states exclusive rights of control within their territories is a commonly accepted one. When investigating how sovereignty should be applied in cyberspace, he concludes that many norms can be easily interpreted in cyberspace as well. However, Jensen also points out that states are hesitant to "accepting responsibility for transboundary harm" (Jensen 2015, 304) originating from their territories. Every state's core sovereignty question is whether it can protect its citizens from internal or external threats. In the physical world, identifying whether a threat originates internally or externally and identifying the appropriate response from the state administration is more straightforward than in cyberspace. Cyber-attackers can be criminal organizations or state-sponsored groups. They can attack companies and citizens in multiple countries at the same time. In other words, cyber-space means new challenges for understanding state sovereignty. Broeders et al. emphasize that evidenced attribution of malicious cyber activities to a specific actor is challenging if not impossible. Such difficulties of attribution make it very difficult to apply evidence-based international law and law enforcement (Dennis Broeders, Els De Busser, and Patryk Pawlak 2020). Dunn Cavelty argues that cybersecurity is "multi-dimensional and multi-faceted security dilemma that extends beyond the state and its interaction with other states" (Dunn Cavelty 2014, 701), forming a foundation for compromise between states and can serve as a basis for cooperation.

This chapter aimed to review relevant literature on debates of the democratic deficit of the EU, as this research aims to contribute to this debate by providing evidence of how the EU works 'for' the people in cybersecurity. This research hypothesises that many aspects of cybersecurity

are more effectively achieved at the EU level, and the cooperation in the field provides values to EU citizens that member states individually would not be able to provide. This research uses the lens of securitization, Europeanization, interdependence, and politicization to investigate this hypothesis.

Methodology

This research aims to understand the added value of EU membership in the field of cybersecurity. To achieve this goal, document analysis and expert interviews were selected as a method. This research focuses on two countries as case studies to allow the required level of focus and depth in the analysis. George and Bennett argue that cases should be selected "to provide the kind of control and variation required by the research problem" (George and Bennett 2005, 83). In the case of the largest EU member states – such as Germany or France - their size and/or global and EU level economic importance, level of digitalization, or other security priorities can impact their approach toward cybersecurity and therefore distort the findings of this research. Also, similarly for smaller states - such as Malta and Luxembourg – due to their size and international diplomatic weight, the cyber exposure could result that findings on cybersecurity advantages of EU membership are also not representative. Due to these reasons, the largest and smallest countries were eliminated from the case selection favouring mid-sized EU member states. The digitalization and socio-economic impacts of ICT drive the importance of cybersecurity for a country: the more dependent a country on ICT, the more vulnerable it is to cyber threats. Therefore, the importance of cybersecurity is more relevant for the country. Therefore, to answer the research question, one highly digitalized and heavily ICT dependent country was selected and one that is less: The Netherlands and Hungary. They are roughly equivalent in size and inhabitants; both are members of NATO and OSCE as well. Membership in security organizations is relevant in this research as NATO itself is also active in cybersecurity defence and response development (North Atlantic Treaty Organization 2020). Since both countries are members of the same relevant international entities (EU, NATO, OSCE), the added value of EU membership should not be impacted by not being a member of other international organizations.

The two selected countries represent different aspects of the European Union in relevant aspects for this research: The Netherlands, which is highly advanced in digitalization, usage of ICT affects all aspects of the society. The country consistently ranks as the top 4th in the Commission's Digital Economy and Society Index (DESI) in the 2015-2020 period[1] (Foley et al. 2020). The Netherlands is also a home of many IT companies, either as a data centre location, a

[1] https://digital-agenda-data.eu/charts/desi-composite

European headquarter of US companies, and as a home and founding country of many globally known online companies and brands (such as Booking.com[2]). Therefore, the Netherlands is representative of the mid-size well developed and highly digitalized northern and western EU member states. Hungary, on the other hand, is less digitalized. It ranks in the bottom 6-8 of the DESI index in the 2015-2020 period[3]. It is not a target neither for any globally relevant foreign or local ICT companies nor home of any global data centre or IT operations location. Since the lower scale of the DESI index mainly contains Central and Eastern European countries, the region in general lags behind in digitalization – Hungary can be considered representative for this region. Also, the different geographical location – one country being on the coast of the Atlantic, the other on the Eastern edge of the EU – contributes different perceptions of external threats or influences. For example, Hungary recently blocked many common EU foreign policy actions called, which was called "hostage-taking of the EU foreign policy" by German foreign minister Heiko Maas recently (Alexandra Brzozowski 2021). This different external threat perception between the two selected countries can be relevant in researching the advantages of the EU in the field of cybersecurity.

This research focuses on the most recent period. The European Union cybersecurity strategy was adopted in 2013 (High Representative of the European Union 2013), and therefore any advantage member states can gain should be in the following period. In order to answer the research question, this thesis intends to build on data gathered from official government documents of the two selected countries and interviews with national experts. The document analysis from the Netherlands and Hungary leverages government documents in local languages[4].

The research focuses on the national approach toward cybersecurity, international cooperation in this field, especially on the cooperation within the European Union and advantages of membership. The source documents are listed in the Bibliography, but the following tables summarize the documents included in the analysis.

[2] https://www.booking.com/content/about.html
[3] https://digital-agenda-data.eu/charts/desi-composite
[4] "All sources originally in the Hungarian language were translated by the author, for whom Hungarian is the first language. All sources originally in the Dutch language were translated by the author, who has a B2 (academic) level state exam (NT2) in the Dutch language."

Table 1 Sources of document analysis – The Netherlands

Document name (English translation)	Document name (original)	Date of issue	Publisher
National Security Strategy 2019	Nationale Veiligheid Strategie 2019	07 June 2019	National Coordinator Counterterrorism and Security, Ministry of Justice and Security (Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Justitie en Veiligheid)
Cybersecurity Agenda - Digital security of The Netherlands	Nederlandse Cybersecurity Agenda - Nederland digitaal veilig	02 August 2019	
Integrated risk analysis - National Security	Geïntegreerde risicoanalyse Nationale Veiligheid	07 June 2019	
Midterm review 2021 - National Security Strategy	Midterm review 2021 - Nationale Veiligheid Strategie	08 March 2021	
National Crisis plan - Digital	Nationaal Crisisplan Digitaal	21 February 2020	
Cybersecurity Landscape in The Netherlands	Cybersecuritybeeld Nederland	29 June 2020	
National Security Horizon Scan 2020	Horizonscan Nationale Veiligheid (2020)	24 November 2020	National Health Institution, Ministry of Health, Wellbeing and Sport (Rijksinstituut voor Volksgezondheid - RIVM, Ministerie van Volksgezondheid, Welzijn en Sport)
The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act		30 July 2020	Tilburg Institute for Law, Technology, and Society, commissioned by the National Cyber Security Centre of the Netherlands

Table 2 Sources of document analysis - Hungary

Document name (English translation)	Document name (original)	Date of issue	Publisher
Government decree 1035/2012. (II. 21.) on Hungary's national security strategy	A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról	21 February 2012	Government of Hungary (Magyarország Kormánya)
Government decree 1163/2020. (IV. 21.) on Hungary's national security strategy	1163/2020. (IV. 21.) Korm. Határozat Magyarország Nemzeti Biztonsági Stratégiájáról	21 April 2020	
Government decree 1139/2013. (III. 21.) on Hungary's national cybersecurity strategy	1139/2013. (III. 21.) Korm. Határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról	21 March 2013	
Government decree 1456/2017 (VII.19) National Info communication Strategy and Digital Welfare Program 2.0	456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról	19 July 2017	
Government decree 1838/2018 (XII.28) Hungary's network and information systems security strategy	Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján)	28 December 2018	

In the case of Hungary, the relevant government decrees were included in the research, the National Security Strategies and the National Cybersecurity Strategies. In the case of The Netherlands, documents issued by the institutions of the Ministry of Justice - the National Coordinator Counterterrorism and Security and National Cyber Security Centrum - were used as primary sources in this research.

The document analysis in both cases focuses on understanding the perception of threat in the cyber field and aims to find the impact of EU membership on national approaches and advantages gained by EU membership. Understanding the perceptions of threat is relevant because, as Stein pointed out, emotions and cognition are complementary in international relations (Stein 2013) and states' willingness to cooperate. Therefore, the advantages gained from EU membership in cybersecurity are impacted if they have a common perception of cyber-threats. Understanding the impact of EU membership on national approaches is relevant because it shows the advantages of EU membership through normalization. Wille defines normalization as a "shift of executive relations towards the political and administrative qualities of the 'normal' model, resulting from a change in existing accountability arrangements" (Wille 2013, 10). In other words, if a piece of evidence is found that the EU impacts national approaches, then then it shows the advantage of the EU membership through driving 'norms'. Such norms can help increasing cybersecurity awareness and resistance in member states. Above the previous 'indirect' advantages, the research also aims to find direct and factual advantages for EU member states, where national governments or institutions explicitly state that a problem is better addressed in the EU level, rather than national approaches. Besides reviewing the official documents, interviews with experts were used to validate and cross-check the findings of the document analysis.

Analysis

The following chapters contain the analysis of the relevant government documents from The Netherlands and Hungary. The analysis focused on identifying unique advantages that these states gain or expect to gain through EU membership. With the cross-border character of cyber-space and cybersecurity, international cooperation in the field is inevitable. Evidence was found to support this in both cases. The analysis focuses on the international cooperation aspect of these states outside the EU if it is relevant to answer the research question. This analysis does not intend to comprehensively review the advantages of international cooperation in cybersecurity for these states, as this research focuses only on the EU aspects.

Findings of the document analysis - The Netherlands

As The Netherlands scores higher in the digitalization index, in line with the expectations, this research found that the cybersecurity topic has higher salience and importance than Hungary's case. Salience and importance are visible through the sheer number of government documents available on cybersecurity and the level of detail and aspects discussed. The Netherlands is a regulation and policy driver in the EU regarding cybersecurity as many of the government documents debate what additional EU level policies would be in the interests of the Netherlands. The cooperation with other EU and NATO members is a core part of the Netherlands' approach towards its cybersecurity.

This chapter reviews the most relevant documents available under the government's (Rijksoverheid) website. The two relevant institutions responsible for cybersecurity are the National Coordinator for Counterterrorism and Security (NCTV) and the National Cyber Security Centre (NCSC). The review starts with the National Security Strategy from 2019 and its midterm review from 2021 - which also builds on the Horizon Scan 2020 document - as these are the 'core documents' to understand how the Netherlands approaches national security. The integrated risk analysis of the Netherlands provides the inputs to the strategic planning as it identifies the risks, including cyber risks to the country. The Cybersecurity Agenda and Digital Security, National Digital Crisis Plan and Cybersecurity agenda documents specifically focus on the cybersecurity

aspects of the Netherlands. The last document is an odd one out as the government did not create that; it is a research study requested by the government. This study is included in the analysis because it demonstrates how the government thinks about or approaches cybersecurity in the European Union context. This document is referred to and can be downloaded directly from the website of a government institution (NCSC), and therefore, this analysis considered it representative to understand the positions of the Dutch government institutions.

National Security Strategy 2019 (National Coordinator for Counterterrorism and Security (NCTV) 2019c)

The National Security Strategy document aims to protect the Dutch society and the democratic order. It categorises the areas of national safety into six categories: territorial, physical, economic, ecological security, social and political stability, and international rule. It acknowledges that though the digital aspect is intertwined in every category, but it argues that due to the confidentiality, availability, and integrity of essential ICT services, this document considers digital safety as part of the territorial security of the Netherlands. A cyber-attack on essential ICT services considered to be an attack on the territory of the Netherlands. It shows the securitization of cyberspace, but it is also in alignment with Jensen's finding as it shows that The Netherlands sees that the state's territorial sovereignty extends to the cyber-space as well (Jensen 2015). The document acknowledges that the cabinet integrates the Cybersecurity Agenda from 2018 in the National Security Strategy.

After the introductions, the document describes the lifecycle of the national security strategy: following the acceptance, government entities execute the necessary actions, which are periodically reviewed, including the review of the threat landscape. The periodical reviews include an additional review of the evolutions of threats. For the cybersecurity topic, it is in the form of the Cybersecurity Landscape document. The chapter discussing national security as a concept starts with the digital safety topic, showing the securitization of cybersecurity, as this is the first topic being discussed. When listing the critical services of the country, the document lists access to the internet – besides the transport and distribution of electricity or drink water – also as critical infrastructure. This categorization shows the dependency of the Dutch economy and society on

online network and information systems. When discussing the international context, the concepts chapter also argues that safety inside the country's borders depends on external security aspects as well; internal and external security is intertwined not just in the physical but also in the digital domain. Therefore, cooperation in the European Union and in a broader international context is important for the country's security interests.

The following chapter reviews the trends that can impact national security. It reviews shifts of international balances of power, such as the impact of tensions between the US and the EU or the increasing assertiveness of Russia or China. It argues that multilateralism can be an effective approach to cyber and hybrid threats or against the risks of extremism and terrorism. As a second point in reviewing international trends, it points out the political instability and that the 'project EU' was never questioned before. The departure of the UK, and the increase of anti-EU parties in countries in multiple member-states (France, Hungary, Italy, Austria, Netherlands, Poland and Sweden), and the degradation of the rule of law in some countries results in the political instability of the EU, which the Netherlands considers a critical part in its national security. The following chapters focus directly on the developments of information technologies and their potential threats to national security. These include the cognitive and autonomous Artificial Intelligence (AI) systems, the increase of the internet-connected smart devices (Internet of Things) that became parts of everyday life. This chapter concludes that society had become dependent on ICT and argues that governance in the digital domain became more and more difficult due to the growing number of large technology companies. It argues that safeguarding public interest can be realized through national and international measures. It also argues that since the EU is looking for strategic autonomy in defence and security, it should include the hardware and software aspects of the critical infrastructures when considering strategic autonomy. In other words, the government acknowledging the interdependence between the national security of the country and the strategic autonomy of the EU. The chapter on economic developments also covers a cyber-related topic: cryptocurrencies. It states that the most significant risks of cryptocurrencies are the criminal or terrorist usage of anonym payment systems, which is why it was included in the EU-level anti-money laundering directive[5]. The government acknowledges that cryptocurrencies can only be

[5] Directive (EU) 2018/843: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843

effectively regulated at an EU level due to the integration and interdependence in the EU. In other words, the question of cryptocurrencies is better regulated at the EU level.

When discussing the dominant risks for national security, hybrid conflicts, conflicts in cyber and information domains are also listed in the first place as part of the chapter discussing undesired interference and influence from external state actors. Later chapters discuss threats from state actors, cybersecurity, disinformation, and digital espionage as the most relevant forms of threats. When discussing multilateral institutions relevant for the security of the Netherlands, EU -including EU defence cooperation - and NATO membership and the trans-Atlantic relations are mentioned as the most relevant ones, explicitly mentioning the cyber domain area as well. Chapter 7 discusses the digital threats, and it mainly refers to the Cyber Security Agenda 2018, where the topic is addressed in more details. It describes the network and information systems security act (Wet beveiliging netwerk- en informatiesystemen - Wbni) - the Dutch implementation of the NIS Directive – as implementing the necessary digital resilience, showing EU directives drive and contribute to the national security. It also calls for the importance of a certification framework for products and services resulting from the European Cyber Security Act.

Regarding new technologies such as 5G and AI, the document emphasizes that the Netherlands is increasingly active within the EU in cybersecurity topics and wants to be a leader in EU level legislation and governance. It also emphasizes the importance of the EU's 'Cyber Diplomacy Toolbox' (Council of the European Union 2017) to prevent cyber-attacks. The Netherlands sees the EU as an option to increase its international diplomatic weight in cybersecurity-related topics through EU membership.

Midterm review 2021 - National Security Strategy (National Coordinator for Counterterrorism and Security (NCTV) 2021), Cybersecurity Landscape of The Netherlands (National Coordinator for Counterterrorism and Security (NCTV) 2020) and the National Security Horizon Scan 2020 (National Health Institution, Ministry of Health, Wellbeing and Sport 2020)

This chapter provides an overview of the analysis gathered from the relevant work documents from the government of the Netherlands, which focus on the developments and changes

in trends that might impact the national security strategy. These focused areas include the developments regarding threatening states, polarization, threats to the critical infrastructures, military threats, and digital threats. The Cybersecurity Landscape describes the developments in the cognitive and automated, and complex IT systems that can lead to technical failures, pointed out by Horizonscan 2020, including new forms of cyber threats originating from these, such as the automated search for vulnerabilities in more advanced ways. Also, as a new form of threats, it points out the impact of cascade effects and risks originating from the dependencies between systems due to linking data and systems. For example, attacks on supply chains can also pose a risk to systems, such as a large scale Distributed Denial of Service (DDoS) on internet services. It also introduces the concept of the cybercrime-as-a-service model where cyber attackers 'provide their services' to other malicious parties. It explicitly mentions the impact of the COVID19 pandemic on cybersecurity as attacks increased against pharmaceutical companies, research centres, hospitals and other care facilities, or malicious actors attempted to gain advantages due to the increased digitalization during the pandemic. The Cybersecurity Landscape document recognises that additional steps were taken at the EU level to improve the digital resilience of the Member States, including the implementation of the NIS Directive, which shows that this document directly considers this EU directive critical for the cybersecurity and national security of the Netherlands. The chapter focusing on the multilateral institutions acknowledges new challenges at the political level as interest are drifting apart. It states that it found social scepticism towards joint action, which questions the added value of the EU membership. However, it argues that partner countries see the importance of a multilateral approach in the cyber domain and uses the cyber sanctions regime from the EU Cyber Security Toolbox as an example. In other words, the government of the Netherlands sees that there are stepbacks in multilateral cooperation. However, it argues that there are depoliticized fields such as the field of cybersecurity cooperation in the EU as an example where multilateral cooperation is unaffected. In other parts, the document reemphasizes the importance of the EU, NATO and UN in the security of the Netherlands, showing the most important international organizations for the security of the country.

Cybersecurity Agenda - Digital Security of The Netherlands (National Coordinator for Counterterrorism and Security (NCTV) 2019a)

This document specifically focuses on the cybersecurity approach of the Netherlands. The introduction lists the key messages: due to the digitalization, cybersecurity is an inseparable part of national security; security in the digital domain is only possible through public-private partnership; knowledge is crucial in cybersecurity; the digital domain is not bound to borders, and the national safety in the digital domain must be considered in a NATO and EU context. This latter shows that, though the national security established the sovereignty claim to the cyber-space too, this document also acknowledges that the Netherlands cannot effectively defend itself in the cyber-space alone. This document also acknowledges the importance of definitions. It provides the government's definition of cybersecurity: "cybersecurity is the set of measures to prevent damage caused by disruption, failure or misuse of ICT and if damage occurs its mitigation" (National Coordinator for Counterterrorism and Security (NCTV) 2019a, 9). The document states that the Ministry of Justice and Safety is coordinating in the government the cybersecurity topic. It also acknowledges that it has aspects that belong to the Ministry of Interior and Kingdom Relations, or the Ministry of Economic Affairs and Climate or the Ministry of Foreign Affairs and that there are also aspects that belong to the Ministry of Defence. The list of ministries involved in the cybersecurity topic supports the arguments that cybersecurity covers multiple policy areas in the administration. The chapter discussing espionage, sabotage and organized crime also refers to the threats from the cybercrime-as-a-service that malicious state actors can leverage for geopolitical gains or to undermine democratic processes. It states that cyberattack from criminal or state actors can undermine the economy of the Netherlands, which also shows the "blurring of boundaries" (Odermatt 2018, 372) between internal, external and defence aspects of cyber-space. When discussing the strategic principles, the document acknowledges the international nature of data- and internet governances and argues that a safer digital domain in the Netherlands can only be achieved through the EU and NATO. It also states that the objectives of the Cybersecurity Agenda of the Netherlands can only be achieved in international legislation, coalition formation and development of international standards, particularly at the European level. It uses the example of the European cybersecurity certification, which it considers necessary to support and stimulate the European Digital Single Market development, as cybersecurity is an inseparable aspect. This

shows two significant findings: the government of the Netherlands acknowledges that the safety of the Dutch cyber-space can only be achieved through international cooperation (interdependence) and that cybersecurity cooperation is an integral part of the European Digital Single Market (spillover and Europeanization).

Further on, when discussing international peace and safety in the digital domain, it emphasizes the importance of the European Union's Cyber Diplomacy Toolbox as a response to cyber-attacks by adding the diplomatic and the economic weight of the EU to the sanctions against cyber-attackers. It also states that to deter potential opponents, the Netherlands has offensive cyber capabilities that can contribute to the developing and making operative cyber-actions in the NATO and EU. In other words, NATO and the EU enhance the Netherlands' cyber-defence and response capabilities. Furthermore, when discussing digital safety of hardware and software products, the document argues for adopting an EU level cybersecurity certification program for ICT products or, in the long term extend the CE[6] marking certification process to include cybersecurity certification as well. This cybersecurity certification of products at an EU level is an essential topic for the Dutch government, as it appears in many documents and studies. Finally, in Chapter 4, when discussing digital processes and infrastructure, the document argues for investigating if additional European or international measures are needed to mitigate impacts of potential disruptions due to a limited number of foreign providers of the digital infrastructure. These demonstrate that the government of the Netherlands considers that multiple aspects of cybersecurity-related governance can be best achieved at the EU level.

Integrated risk analysis (National Coordinator for Counterterrorism and Security (NCTV) 2019b)

This document is the risk analysis that is used as an input in the national security strategy. Though its findings are incorporated into the national security strategy, this document was included in this analysis as it provides insights into the threats that the government identified. When identifying themes and risk categories, the risk analysis dedicates its own theme to cyber

[6] https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm

threats, showing that the government considers it equivalent to other themes such as natural disasters, threats to health and environment, and fiscal-economical threats, or threats to international peace. Within the cyberthreats theme, it identifies four risk categories: digital sabotage, threatening the functioning of the internet, cyber-espionage and cyber-crime. This own dedicated theme and focus show the securitization of cybersecurity. When discussing these in detail, the document acknowledges that cyber-threats can cover a wide range of policy areas, and threats from cyber-space can be the means or goals of an attacker as hybrid threats. It names Russia and China explicitly as most likely sources of cyber- and hybrid threats. The document explicitly states that the two main organisations to safeguard the Netherlands' security interests are NATO and EU, and risks threatening these organizations implicitly mean threats to the Netherlands. The EU is described as a broad security actor with a role in domestic security aspects and ensuring security in the EU neighbourhood, while NATO provides collective security guarantees. In other words, this risk analysis considers that the EU is an integral part of the safety of the Netherlands in the Justice and Home Affairs (JHA) and internal security areas, while the other documents also refer to the Cyber Diplomacy Toolbox - and not only NATO - as an important EU tool in external security. However, it must be noted that the relevant chapter in the risk analysis talks about the EU and NATO in general and not specifically in the cybersecurity context.

National Crisis Plan – Digital (National Cyber Security Centre (NCSC) 2020)

The purpose of this document is to provide an overview of the national arrangements and action plans to control incidents related to the security of networks and information systems. The plan describes the relevant connections between involved public and private entities in different cybersecurity-related incidents. The incident types are categorized depending on different parameters. These include intent (non-intentional, intentional), source (internal or external), actor (state or non-state), impact (only ICT, important social impact, critical infrastructure), impact region (one safety region, multiple-safety regions, multiple countries) and whether a technical solution is known or unknown. Chapter 3 lists the process steps and actors and contains the following figure on the cyber-incident crisis management structure:

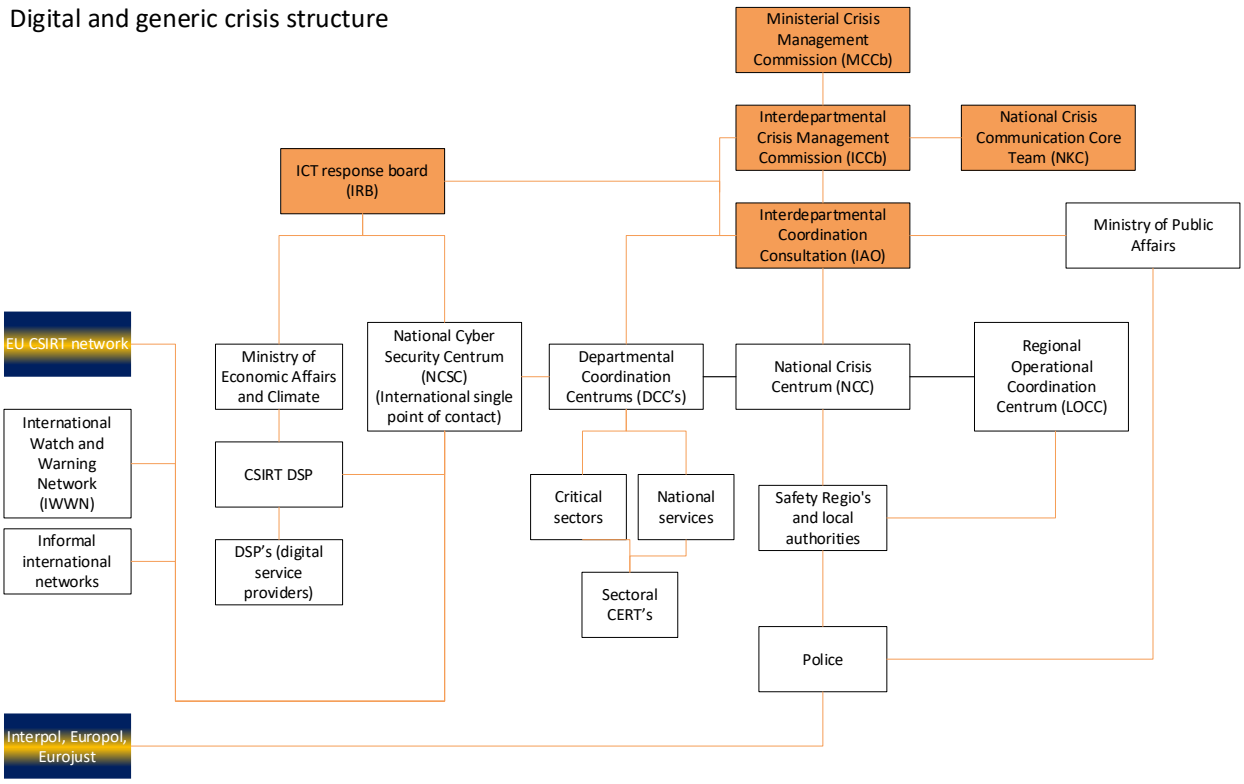

Figure 1 Digital and generic crisis structure. Source: (National Cyber Security Centre (NCSC) 2020, 32)

This figure shows that the Netherlands considers the operative cooperation with EU bodies (the EU Computer Security Incident Response Teams (CSIRTs) supported by ENISA, Europol and Eurojust) as an integral part of the cybersecurity crisis management process. Since the Dutch Police and the NCSC directly communicate these EU agencies - and not through a diplomatic channel – it allows an operative, depoliticized and prompt cooperation between experts. Such cooperation is essential when dealing with cybersecurity incidents, as the situation in the cyber-space can change fast and prompt sharing of information - without the need for approvals - between the national agencies can be crucial in effective crime-fighting. The EU provides the required trusted environment that enables this operative cooperation between national agencies and experts possible. This way, the EU provides the necessary, trusted environment and a daily operative environment that makes fighting cyber-crime or cybersecurity incidents more effective for the member state agencies. This way helps to make the cyber-space more secure for the citizens. The document also acknowledges the importance of CERT-EU, ENISA, Europol (European Cybercrime Centre - EC3), Eurojust (European Judicial Cybercrime Network). It gives practical examples of how these EU agencies and the Commission helps member state with cyber incident

management. Examples include ENISA's twice a year Cyber Europe practice exercises or that the Commission provides blueprints on cybersecurity incident management for member states. When discussing tactical and strategical cooperation, it emphasizes the importance of 'Like Minded' states within the EU as an important foundation for operative cooperation. Regarding the EU, it also mentions that the importance of the CFSP and cybersecurity sanctions in the Cyber Diplomacy Toolbox and that the Permanent Structured Cooperation (PESCO) also has cybersecurity aspects. It uses the example of a Lithuanian led project[7] that aims to improve the response capacity of participating member states in deploying support at cyber crises. "In this way, the project contributes to better cooperation in the field of cybersecurity between member states and thereby a digitally safer Europe" (National Cyber Security Centre (NCSC) 2020, 55). This quote from the National Crisis Plan confirms the previous findings and explicitly states how cooperation within the EU member states contributes to citizens' safety. When discussing the OSCE and NATO, the discussion and role of these organizations described only in general, and the document does not provide examples of direct daily operations in these organizations. Regarding NATO, the document emphasizes NATO's importance in deterrence in cybersecurity and hybrid warfare.

The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act (Irene Kamara et al. 2020)

This study was created by the Tilburg Institute for Law, Technology and Society and was commissioned by the National Cyber Security Centre of the Netherlands (NCSC). Though this document was not created by a government entity - but for one - since it is published on the website of the NCSC, it is considered to be representative of the government's position, especially that many previously discussed government documents also emphasized the importance of the cybersecurity certification. This study aims to examine how the Dutch cybersecurity certification landscape responded to the EU Cybersecurity Act and whether any intervention from NCSC would be required. It provides an overview of the legal framework on cybersecurity in the Netherlands and the EU, the cybersecurity certification in the Netherlands and provides potential roles for the

[7] Cyber Rapid Response Teams and Mutual Assistance In Cyber Security (CRRT) https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cybersecurity/

NCSC. It mainly focuses on the Dutch implications of the EU Regulation 2019/889[8] on 'ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act - CSA)'. One of the document's findings is that "Certification bodies are interested to follow the EU CSA developments and participate in the development of the upcoming cybersecurity certification schemes, for instance by joining the ENISA ad hoc working groups" (Irene Kamara et al. 2020, 33). It also states that "Collaboration in these European platforms is also important because equipment is bought on an international market and European solutions are deemed desirable to ensure the devices are of adequate quality and security" (Irene Kamara et al. 2020, 40). Through these examples, the document demonstrates how EU CSA and ENISA facilitates collaboration and sharing of information and experiences between experts, improving the quality of results and facilitating safer cyberspace.

Analysis of the findings – The Netherlands

The high level of digitalization in the Netherlands resulted in high dependency on ICT and therefore meant significant exposure to cyberthreats for the country. Cybersecurity is the first chapter in the national security strategy of the Netherlands, which not just shows the importance of the field but also the securitization of the topic. When discussing ways to mitigate cyber threats, the government of the Netherlands considers its international cooperation in the EU and NATO an integral part of its national actions, as cybersecurity by nature is cross-boundary. The National Crisis Plan for digital security of the Netherlands considers the EU agencies, such as Europol, EU CSIRTs, CERT-EU, ENISA, as a 'logical extension of national agencies' and considers them an integral part of the cybersecurity incident management.

At discussions with cybersecurity experts, it was pointed out that the majority (the estimation was 70%) of the Dutch cybersecurity laws are implementation of an EU directive. However, this high number of cybersecurity-related legislation originating from the EU does not mean that the Netherlands 'simply just adopts' EU law, but rather acknowledges that national approaches would not work or would not be adequate due to the interdependence. The research

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1623773945297

also found explicit evidence where the government of the Netherlands states that it aims to be a leader in cybersecurity regulation at an EU level, further confirming this finding. The recent focus area of the government of the Netherlands is the EU level cyber-certification of products and services, potentially extending the CE marking – 'conformité européenne', used to demonstrate compliance with EU product regulations - with also cybersecurity criteria.

The findings also confirm the multi-policy aspects of cybersecurity, as the government of the Netherlands discusses in details the internal, external and defence policy aspects of cybersecurity. The internal policy aspect focuses on JHA cooperation, enabling effective police and judicial actions to fight cross-border cybercrime. The documents express the phenomenon of cyber-crime-as-a-service when cybercriminals offer their services to other malicious actors, including nation-states. Here EU can complement NATO: while NATO cooperation focuses on defence cooperation and deterrence, the EU facilities cooperation necessary to fight cyber-crime, which can be blurred between cybercriminals and nation-states. The analysis found evidence on the importance of the EU's regulatory power compared to NATO and the importance of the Cyber Diplomacy Toolbox, as it provides different diplomatic instruments – through economic sanctions – that can be more effective. NATO would be able only to provide a military response, while the EU Cyber Diplomacy Toolbox can be easier engaged and leveraging the economic power of the EU, it can be still very effective. The discussions with cybersecurity policy experts regarding the Cyber Diplomacy Toolbox emphasized the importance of the ability to share information in a trusted environment in an operative manner.

Findings of the document analysis - Hungary

This chapter contains the findings of the document analysis of the government decrees on Hungary's national security strategy and national cybersecurity strategy. The document analysis was complemented with an interview with a diplomat at the Hungarian permanent representation to the EU to validate and check findings. This research found that Hungary somewhat lags behind the Netherlands in the sophistication of cybersecurity policies. While the Netherlands is more aims to be the leader in the EU in the cybersecurity governance field, Hungary is more of a follower in this area. Therefore, due to the more limited type of government documents available, to widen

the overview and gain better context, this research also extended the review to previous versions of the national strategy documents related to cybersecurity.

Hungary's first cybersecurity-focused national strategy dates to 2013, which was revised in 2018. The following figure summarizes the primary sources being reviewed. The documents are visualized in a timeline. The arrows represent when a document is referred to in a later one. The NIS directive is placed on the figure to put it into context and indicate its influence on the different government decrees.

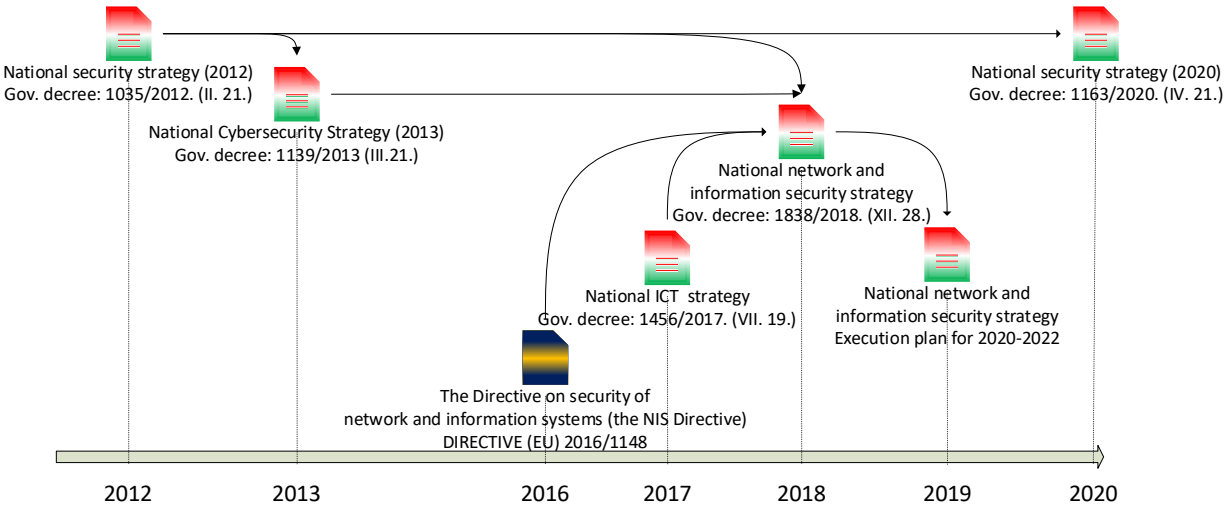

Figure 2 Timeline of the Hungarian Government decrees related to cybersecurity

The review of the primary sources starts with the Hungarian national security strategy from 2012 and the latest from 2020. These were included in the analysis because the Hungarian cybersecurity approach was only derived from the national security strategy before the NIS directive. Furthermore, even though the current 2018 Hungarian cybersecurity strategy predates the 2020 Hungarian national security strategy, the latter also contains cybersecurity references. As the figure shows, the current centre for cybersecurity strategy in Hungary is the 1838/2018. (XII.28.) government decree on network and information security. This decree replaced the previous 2013 cybersecurity strategy and incorporated the inputs from the NIS directive and the national information communication technology strategy and the EU cyber security strategy.

Government decree 1035/2012. (II. 21.) on Hungary's national security strategy (Government of Hungary (Magyarország Kormánya) 2012)

The 2012 Hungarian national strategy reviews the national goals, government tasks, and tools required to carry out Hungary's national security interests. The strategy emphasizes the changing nature of national security and places it in an international context in which globalization and integration result in new threats. It considers armed conflicts for Hungary highly unlikely but acknowledges other forms of armed attacks - such as international terrorism – that can still threaten Hungarian national security. It mainly focuses on other forms of threats than cyber when assessing threats, which shows the lack of securitization of the cybersecurity topic in 2012. It explicitly emphasizes that Hungary views multilateral[9] cooperation within the UN and the OSCE as important to national security. It derives Hungary's national security from the county's NATO and EU membership. Regarding NATO, it emphasizes the importance of Article 5, and regarding the EU membership, it states that cohesion and solidarity are the only way Hungary can face the security challenges of the 21st century.

Only Article 31 focuses explicitly on cybersecurity. It acknowledges the importance of ICT in Hungary's economy, social and civil administration, and security. It recognizes that the technological advancements made it accessible not just to states but to non-state actors – it names terrorist groups – to execute attacks and disrupt communication systems. It also recognises that ICT tools can be used by criminals as well. Regarding cybersecurity, the 2012 Hungarian national strategy names two sets of actions for the government to act on: first is a continuous assessment and analysis of cyber-threats, enhancement of coordination within public authorities, the importance of increased social awareness and leveraging the advantages of international cooperation. The second action item it names for the government is the enhancement of defence capabilities of critical infrastructure components. Regarding the latter, the strategy explicitly points out the importance of EU cooperation in the field of cyber-defence. These are both quite generic and high level, lacking any tangible action.

The EU Cyber Security strategy (High Representative of the European Union 2013) was published in February 2013; therefore, this document predates it. Though there were international

[9] Author's note: The original document uses the '*multilaterális szervezetek*' expression which translates to *multilateral organizations*

examples of cyber-attacks - such as the 2007 Estonian cyberwar (Kaiser 2015) – as this document shows, the topic was not yet salient, and the securitization of the cybersecurity topic happened.

Government decree 1163/2020. (IV. 21.) on Hungary's national security strategy (Government of Hungary (Magyarország Kormánya) 2020)

The introduction of this government decree refers to the 2012 strategy and argues that the new multipolar world order[10] and changes in global security challenges require revision of Hungary's national strategy. Important to note that this document uses the 'multipolar' expression and not the multilateral, mainly used by western states. This change of wording can indicate a shift in the orientation of the Hungarian government. Whether or not this change of wording intends to indicate a change in foreign policy objectives, when Hungary assesses security threats, it considers the NATO and EU strategies foundational to the national interest. Similarly, like the 2012 strategy, it names the UN and OSCE and adds the Council of Europe as a forum for representing Hungarian national interests. Article 31 and 46 emphasizes the importance of protection against hybrid threats and names cooperation between military, law enforcement and civil defence capabilities in defence to fight against hybrid threats. Article 32 states that the Government of Hungary makes all necessary steps to protect against cybersecurity challenges and that the corresponding national capacities must be developed. When comparing this to the 2012 national security strategy's cybersecurity aspects, this increased salience on cyberthreats and cybersecurity shows that by 2020 this topic is securitized.

Further, this document names the continuous sophistication of cyber-attacks and lack of end-user awareness as crucial challenges in cyber-defence capabilities when discussing primary sources of threats. Articles between 69-72 explicitly mention the increased dependency on ICT in the private and public sectors, further increasing vulnerability to cybersecurity challenges. It acknowledges that the number of state and non-state actors increased who leverage the cyber-space to cause damage - even in the physical world - and expects that the importance of cyber-space in

[10] Author's note: the original document uses the Hungarian phrase "*többpólusú világrend*" which translates to *multipolar world order* and not "*többoldalú*" nor "*multilateriális*" expressions which would be *multilateral* as used by the 2012 national strategy or by the documents from the government of the Netherlands.

warfare will further increase. Article 124 c) and d) points describe combined diplomatic, cyber and secret service operations, monetary and economic pressures combined with military threats as a form of hybrid security threats which can cause not just cyber but physical world damages as well. Though not explicitly stated, this wording means that Hungary considers cyber risks part of the territorial security, similarly to the Netherlands. Article 76, 79 and 154 states that the lack of legalization of crypto-currencies - which cyber-criminals can leverage - also poses a threat to national security. This way, the national security strategy also acknowledges the defence and the criminal threat aspects of cyberspace, showing that Hungary also considers it a multi-policy area. Article 33 states that Hungary is highly integrated into the global and European value chain, which - due to the intertangled nature of the European economy - poses threats if one member is compromised that exposes the others as well. In other words, the Hungarian government acknowledges interdependence in the field of cybersecurity between European member states. Articles between 93-96 focus on cooperation in the European Union. These articles explicitly state that besides NATO cooperation, the cooperation within European Union is also in Hungary's foreign and security policy interest and shows the EU is an integral part of it. When identifying responses and actions, Article 135 names the Hungarian military that must be able to respond to security threats in land and air and in cyber-space as well. Interestingly compared to the Netherlands, Hungary emphasizes the military's role in cyber defence as well.

Article 151 also states that responding to cyber-crime, the Hungarian law enforcement agencies and secret services must increase cooperation with European Union member state partners, recognizing the values gained from cooperation in the EU. Even though earlier the military aspects of cyber-defence were emphasized, Hungary also recognises it as a JHA area where cooperation in the EU has a significant aspect. Articles 159-165 identifies actionable items for cyber-defence: coordination within different branches of the government and public authorities, development of military and law enforcement capabilities, international cooperation including the development of international laws to regulate cyber-space, national research and development, protection against disinformation. These show that cybersecurity covers the multi-policy areas in the administration.

Comparing the 2012 and 2020 national security strategies

When comparing the 2020 Hungarian national strategy with the 2012 version from the cybersecurity and cooperation in the European Union aspects, the following conclusion can be drawn: increased importance of cybersecurity and international cooperation, especially with European Union member state partners. While the 2012 strategy contains only one article (186 out of 5813 words or 3,3% of the strategy) explicitly focusing on cybersecurity, the 2020 strategy contains 22 articles (1186 out of 11419 words or 10,3% of the strategy) explicitly focusing on cybersecurity, showing the securitization of the topic. It would be a mistake to contribute this securitization only to the EU - as many technological advancements, political and international incidents relating to cyber happened after 2013 - however, the evidence shows that Hungary sees value in EU level cooperation in the field of cybersecurity. Though the 2012 strategy also emphasizes the importance of international cooperation on security matters, it only generally talks about the UN, OSCE, NATO and EU, emphasising the latter the least. The 2020 strategy explicitly calls out the importance of cooperation with EU partners in the cybersecurity field, especially in the field of cyber-crime (Europol) and hybrid warfare, also showing the Europeanization of the topic.

Government decree 1139/2013. (III. 21.) on Hungary's national cybersecurity strategy (Government of Hungary (Magyarország Kormánya) 2013)

Compared to the national strategy documents, the 2013 cybersecurity strategy is significantly shorter, only four pages. It derives its legal justification from Article 31 of the 2012 national security strategy and Article 38 of the Hungarian constitution, which describes the importance of the state's role to protect its territory. Again, similarly, like the Netherlands, cyber threats fall into the category of territorial threats. It refers to international laws as its basis for this. These include the 2001 Convention on Cybercrime (also known as the ‘Budapest Convention’) (Council of Europe 2001), the recommendations from the European Parliament resolution 2012/2096(INI), the European Cybersecurity Strategy 2013 and the NATO’s Strategic Concept. Article II/7 states that Hungary’s national interest is cooperating with any state and non-state actors

who share similar values. It mentions the importance of the EU, NATO and OSCE, the UN and the Council of Europe as a forum for this cooperation, however just in general terms. There is no apparent order or preference for specific forms of cooperation, and no clear examples are given. Besides these organizations, the strategy also mentions the importance of regional cooperation between the central and eastern European region in cybersecurity areas, without any specific details. It emphasises the importance of the implementation of the European Union Digital Agenda and the NATO cybersecurity policy. When discussing the institutions for European cooperation, the strategy names the Body of European Regulators for Electronic Communication (BEREC) and the European Union Agency for Network and Information Security (ENISA) as forums for cooperation with EU member states, which already shows some level of Europeanization in the cybersecurity field. Although Hungary had a cybersecurity strategy in 2013, it was pretty short and unfocused, showing that the topic was not yet securitized.

Government decree 1838/2018 (XII.28) Hungary's network and information systems security strategy (Government of Hungary (Magyarország Kormánya) 2018)

The 2018 National cybersecurity strategy explicitly names the previous 1139/2013 cybersecurity strategy as a predecessor and positions the new strategy as necessary because of changes in cyber-space, new cyber threats and changes in the international landscape, showing the securitization of the topic. With its 28-page length, this is a significantly more detailed document than its 2013 predecessor. It identifies the following aims: improve intra-government cooperation, increase international cooperation, the joint responsibility of public and private actors, improve educational and research programs, increase awareness, which shows similarities with the Dutch cybersecurity strategies. It also explicitly refers to 2016/1148 (EU) NIS directive, further showing Europeanization. Similarly, like the 2013 strategy, it also names the Budapest Convention, the 2010 NATO strategy concept, and the EU cyber-strategy as international bases for the national cybersecurity strategy. As an important new aspect - similarly to the Netherlands - it provides definitions for cyber-space, cybersecurity, security incidents, and network and information systems to establish a common language with EU/NIS terminology, further proving the Europeanization. It refers to Eurostat findings on cybersecurity and identifies that both Hungarian

small- medium and large enterprises are behind the EU average on preparations against cyber threats. This way, the Hungarian government uses this Eurostat data to operationalize cybersecurity and the country's resilience, showing the Europeanization of the topic. It argues that based on the experiences of the last five years - since the previous cybersecurity strategy - the international cooperation with EU members and other international partners was a high priority. It concludes that there was a significant improvement both within the institutional setup and the law enforcement and crisis management and response capabilities at the EU level, acknowledging the added value of the EU. It contains a detailed description of the Hungarian institutions that play a role in cybersecurity, including government and non-government actors. When discussing the identification of the Hungarian critical infrastructures, it refers to the 2008/114/EC[11] Council directive for defining critical infrastructures, showing the EU impact as well. When discussing the importance of public awareness, it refers to the 'Safer Internet' and European cybersecurity campaign organized by ENISA as the most important forum for enhancing the Hungarian public awareness, showing the importance and added value of EU agencies. When discussing cyber-crime action items for Hungary, it states the importance of Hungarian law-enforcement agencies involvements in international cooperation. Chapter 1.4 states that EU members' Computer Security Incident and Security Response Team (CSIRT) and Computer Emergency Response Teams (CERT) must coordinate. This cooperation allows protecting private-owned critical infrastructure components or civil services (such as banking) cross border as well, showing the importance of EU level cooperation and the added value of the EU in managing cyber incidents. It also states that Hungarian institutions actively cooperate in sectoral CSIRT and Information Sharing and Analysis Centres (ISACs) at the European and international level (action items 28 and 29).

Comparing Hungarian cybersecurity strategies

Hungary's first cybersecurity strategy was created in 2013 and was only four pages, referencing international or EU level cooperation only in generic terms. Although the 2018 cybersecurity

[11] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

strategy builds on the same 2012 national security strategy as the 2013 cyber-strategy, the latter is more mature. It has more detailed information, definitions, and describes specific actions, showing that by 2018 the topic was securitized. The 2018 cybersecurity strategy strongly leverages EU membership to establish baselines and operationalize or leverage information and best practices sharing, including awareness training and campaigns by ENISA. These are values of the EU membership that Hungary does not get through any other form of international cooperation. The 2018 strategy also leverages methodologies and requirements from the NIS directive when assessing and determining necessary protections for critical infrastructures, showing Europeanization. It also includes actions for international cooperation with a specific focus on actions for cooperation within the EU through ENISA. From these, we can conclude that EU membership was a catalyst; it helped to increase the maturity of the Hungarian cybersecurity administration by providing a basis for assessment and by defining actionable items and requirements – such as the need to assess critical infrastructure or to set up national CERT and CSIRT organizations – where the public administration needed to improve. Interestingly while cooperation and importance of cyber-crime matters are mentioned with a strong emphasis in the (latter) 2020 national strategy, the 2018 cybersecurity strategy does not cover the cyber-crime aspect. Reviewing Hungary's national cybersecurity strategies roles of ENISA and the NIS Directive shows evidence on Europeanization: these played an important role in education and built awareness for Hungarian cybersecurity experts, both through its coordination role and through cybersecurity exercises it helps to facilitate.

Analysis of the findings – Hungary

This chapter reviewed Hungary's national and cybersecurity strategies to investigate the added value of EU membership to Hungary. The 2020 national security strategy has significantly increased its focus on cyber areas than the 2012 one that pre-dated EU cybersecurity strategies. The increased attention in the latter is evidence of securitization of the cybersecurity topic. Furthermore, the focus is on practical and operative cooperation in the EU, such as Europol or CERT/CSIRT cooperation and that Hungary operationalizes Eurostat data for measuring cyber-resilience and readiness, which are evidence of Europeanization. These findings were confirmed

in an interview with a Hungarian diplomat working in the EU. When discussing the EU membership advantages for Hungary on cybersecurity matters, he emphasised the importance of the new EU Cybersecurity strategy (European Commission 2020b) and the Council Conclusions on it[12] and how those provide valuable input for the national approach. Further, he also confirmed the importance of EU led cooperation such as the Computer Emergency Response Teams (CERT)/Computer Security Incident Response Teams (CSIRT) cooperation of national teams[13], the role of the ENISA and the Commission's proposal on the EU-CyClone Network[14] for cross-border cyber incident responses, which also further contribute to the cybersecurity of Hungary. When comparing the added value for Hungary between NATO and EU membership in the interview, the answer was:

> "*EU allows wider and deeper cooperation, especially when it is necessary to define EU-wide responsibilities and obligations. The EU membership makes it possible to coordinate several tangible and operational policy areas. NATO is important in transatlantic relations, but it is mainly organized around Article 5; it offers less policy or diplomatic tools to address common cyber challenges and more joint exercises, dialogues and information sharing. Such deep operative cooperation could be based on voluntary information sharing between EU member states.*"

This statement confirmed the findings from the Dutch National Crisis plan and Hungarian national strategy from 2020, that operative, daily cooperation in cybersecurity and the legislative nature of the EU matters in cybersecurity. Fighting cross-border cybercrime is enabled by the EU, while NATO mainly focuses on deterrence and joint defence. This way, the EU contributes to safer cyberspace, as it covers multiple policy areas, which is essential due to the multi-policy area nature of cybersecurity. Since the EU covers policies relevant to the operation of the single market and that it has JHA aspects as well, it allows it to be effective in helping member states to fight cybercrime. EU agencies provide a trusted operative environment where information sharing is possible. This way, the EU facilitates an environment where member state agencies can 'put their

[12] Adopted on 22 March 2021
[13] https://csirtsnetwork.eu/
[14] https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

pieces of the puzzle together' and achieve better results than individually. The interview also confirmed that from the member states' point of view, the proposed NIS 2 directive (European Commission 2020a) would provide new advantages and new elements, such as that the ENISA will maintain a centralized vulnerability disclosure registry. This centralized registry will allow a new level of cooperation and information sharing between member states: if a technical vulnerability or exploit is found by one member state agency, it will be made available to others, helping them build cyber resiliency against or better fight cybercrime. The interview also pointed out the capacity building, training, raising awareness and strengthening security culture facilitated by ENISA and EU agencies, as these also directly contribute to the cybersecurity of Hungary.

The interview revealed an interesting finding of the CFSP aspects of cybersecurity and the Cyber Diplomacy Toolbox. Although Hungary is often seen vetoing in joint actions in CFSP and blocking common actions, the opinion expresses in the interview focused on how the Cyber Diplomacy Toolbox provides the member states with a wide range of diplomatic tools to coordinate joint responses on foreign-related cyber incidents. Such diplomatic response could contribute to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. In other words, the Cyber Diplomacy Toolbox – leveraging the economic and diplomatic weight of the EU – contributes to the cybersecurity of countries such as Hungary. This also confirms the findings of the Dutch Midterm review document, which stated that despite the stepbacks in multilateral cooperation in the EU, the Cyber Diplomacy Toolbox is successful, and the cooperation in this field is intact, as member states see the EU's added value to the cybersecurity. The attribution is a challenging aspect of the diplomatic response. The most crucial factor is information sharing – every member state and agency can add their piece of the puzzle – which is only possible in a well-connected relationship that facilitates the required trust. A proper attribution – identifying a malicious actor behind an attack – would be a lot more challenging, if not impossible, without information sharing and a joint assessment. Even though attribution to a State or a non-State actor remains a sovereign political decision, cooperation within the EU provides access to information that would not be available. Also, this information sharing enables joint action, such as sanctions as part of the Cyber Diplomacy Toolbox, which, if done at the EU level, has greater international weight than what member states individually would achieve.

Discussions

This research aims to investigate the added value of the EU membership to contribute to the academic debate on the democratic deficit of the EU. The main EU contribution to cybersecurity is directives (such as the NIS and NIS2 directives) or regulations (such as Cybersecurity Act) that follow the same ordinary legislative procedures as legislation in any other EU policy area, making them no different a democratic control points of view. This research found that for both The Netherlands and for Hungary, the EU's Cyber Diplomacy Toolbox provide benefits, which is a tool in CFSP coordinated by the EEAS and the Council of the European Union, which allows even less democratic control by the people as the Council is the most intergovernmental entity of the EU. Therefore, in the arguments of Weiler and Hix (Simon Hix 2008; Weiler 1995), the cybersecurity policy of the EU is even less democratic than any other EU policy areas. The only democratically elected body – the European Parliament – has no control over one of the significant aspects -the Cyber Diplomacy Toolbox - that was found to be highly beneficial to the member states investigated. However, none of the EU legislations nor the Cyber Diplomacy Toolbox are redistributive in nature. Therefore it can be argued that as Moravcsik, Majone and Scharpf (Majone 1998; Moravcsik 2002; Scharpf 1999) pointed out, the EU's democratic deficit should be investigated from a 'for' the people aspect. This research found that the administrations of both countries see direct and tangible advantages of the cooperation in cybersecurity matters within the EU, and both administrations consider operative cooperation within the EU an integral part of their national cybersecurity approaches. This finding supports Richard Bellamy's argument that depoliticizing and even come cases by limiting democratic input 'by' the people can be justified for the advantages of more effective output that deliver results 'for' the people (Zimmermann and Dür 2016, 65–72). In the field of cybersecurity, the EU provides direct and tangible benefits to the citizens of the member states. Such examples include help fighting cybercrime, ensuring the proper security of hardware and software used, helping states in attributing cybercriminal actors, and limiting further malicious activity through sanctions or enhanced interest representation. These all directly beneficial 'for' the people. Due to digitalization – especially with the accelerated dependency on online technologies because of the COVID pandemic – cybersecurity has actual, physical world implications as well. Therefore, the

effectiveness of the EU in the field of cybersecurity contributes not just a safer cyberspace, but to traditional safety and security to citizens as well.

Majone argued that EU policies should either solve specific problems or serve the integration objectives (Majone 2005). The cross-border nature of cyberspace and the fact that due to digitalization, many areas of life depend on cybersecurity 'makes it inevitable' that like-minded states, who already share common policies in many other areas, integrate their efforts in cybersecurity. Both states in this research consider the information sharing and operative cooperation in a trusted EU environment crucial for their national security. They view the EU agencies (Europol, ENISA, CERT-EU) as a 'logical extension' of their corresponding national agencies. Therefore, in the field of cybersecurity, the EU policies solve specific problems through further integration. The legislative aspects (NIS directive, Cybersecurity Act, JHA cooperation) of the EU level cybersecurity cooperation can be viewed as mainly a result of spillover due to the 'four freedoms' of the single market. The Cyber Diplomacy Toolbox as part of the CFSP is intergovernmental by nature, yet member states found that only integration of intelligence (for attribution) and joint action can help mitigate external cyber threats. These findings support the arguments of Samonek that Europeanization is playing a significant role in cybersecurity (Samonek 2020), both in supranational and in intergovernmental aspects.

The findings of this research contradict Mats Peterson's arguments that the EU is inefficient to adapt to the challenges of the globalized world. (Zimmermann and Dür 2016, 37–42). Despite the frequent vetoes of common CFSP positions or rejection of common actions at the EU level by Hungary, the country still finds cybersecurity cooperation - including the Cyber Diplomacy Toolbox in CFSP - an essential asset for national security. The importance of the Cyber Diplomacy Toolbox shows that Hungary sees the EU as an effective way to respond to globalized challenges presented by cyber threats and that cybersecurity cooperation is depoliticized. The fact that both countries recognise the importance of cybersecurity cooperation also supports the arguments of Samonek that building cybersecurity resilience at the EU level is more effective (Samonek 2020). This finding on the Cyber Diplomacy Toolbox partially contradicts the findings of Fuchs, who concluded that politicization and interdependence would drive the EU cybersecurity agenda (Fuchs 2018). This research found that despite the political contrasts between The Netherlands and Hungary in other fields, the cybersecurity cooperation is depoliticized, and the cooperation is frictionless. However, the research found evidence that supports Fuchs' argument as

interdependence both in the legislative (supranational) and CFSP (intergovernmental) aspects of cybersecurity is a key driver in integration.

The evidence found supports the arguments of Carrapico and Barrinha (Carrapico and Barrinha 2017), that the EU is becoming a more and more important actor in cybersecurity. Both countries emphasize the importance of NATO's Article 5 as a key pillar in their national security, but operative cooperation and developments are mainly happening in the EU. The Netherlands explicitly states that it aims to be the leader in driving EU policies and legislation in the field of cybersecurity and defines its national strategies and actions in an EU context. Though Pernik argues that NATO is more successful than the EU in a comprehensive approach to cybersecurity (Piret Pernik 2014), her research predates the NIS Directive, the Cybersecurity Act and the Cyber Diplomacy Toolbox, which as found by this research are the most relevant aspects. Though this research focused only on two member states, it found direct evidence that these states aim to achieve their cybersecurity goals leveraging the advantages of the EU. Both states consider the EU level legislation, agencies and cooperation a cornerstone and integral part of their national approaches towards cybersecurity. This contradicts the findings of Sliwinski (Sliwinski 2014), as the cybersecurity cooperation is happening in the EU institutional framework, and not the member states dominate the future of cybersecurity or through EU level cooperation. A further argument in line with Carrapico and Barrinha and confuting Pernik and Sliwinski[15] is that the operative and legislative nature of the cooperation in the EU provides more sophisticated and precise response options - such as economic sanctions, EU legislation- to member states. Such sophisticated response options contributes significantly more to the operative cybersecurity of the member states than the potential military response and deterrence that NATO could only provide. In other words, since NATO's response can only be military due to its nature, states are less willing to use that than leveraging non-military options – for example, economic sanctions – as responses to cyber incidents. NATO was founded for territorial defence; the EU was founded for preserving peace and achieve mutual benefits through operative cooperation and supranational legislation. Since cyber threats cannot be stopped at the borders, attribution and effective cyber crime-fighting and

[15] The works of Pernik and Sliwinski are from 2014 and therefore predate the 2016 NIS directive and 2017 Cyber Diplomacy Toolbox which are the main pillars of cybersecurity in the EU. This shows that the EU level activity and Europeanization of cybersecurity started after 2014.

prevention requires operative cooperation, the EU is in many aspects better suited to contribute to cybersecurity to its members.

The original hypothesis of this research was that the EU contributes to the member state's cybersecurity through Europeanization and securitization. Furthermore, as Christou's and Tikk and Kerttunen stated (Christou 2019; Tikk and Kerttunen 2020), this research also found evidence on the securitization of cybersecurity as the topic is highly salient in the current national security strategies of both countries. However, the results of this analysis do not provide enough evidence on whether this securitization of cybersecurity is related to the EU and the increased activity and awareness at the EU level or whether it is due to other trends or external events. Nevertheless, the analysis found that as Fuchs and Samonek (Fuchs 2018; Samonek 2020) stated, Europeanization and interdependence are playing a significant role in the cybersecurity cooperation and legislation in the case of these two member states.

Conclusion

This research aimed to investigate the added value of EU membership in the field of cybersecurity, with the aim to determine if the EU contributes to the safety and security of the member states in a way that no other form of international cooperation is capable. This research aims to contribute to the academic discussion on the democratic deficit of the EU, as Moravcsik, Majone, and Scharpf argue that what the EU represents is the democracy 'for' the people (Majone 1998; Moravcsik 2002; Scharpf 1999). They argue that the EU's democratic values can be derived from the fact that it provides values to its citizens that member states alone would not. By reviewing the case studies of the Netherlands and Hungary, this research found evidence that the EU provides and facilities a trusted and operative environment that allows a more profound and broader collaboration than any other form of international cooperation. Compared to NATO, the EU's advantage is that it covers multiple policy areas, not just defence and deterrence. This legislative aspect of the EU found to be extremely important in cybersecurity. Both countries consider the EU and NATO core to their national security, as they complement each other.

The research found evidence for the securitization of cybersecurity both in the internal and external security of the states. Cooperation within EU agencies (mainly in Europol and ENISA) is an integral part of policing and judicial cooperation of both countries. Fighting cybercrime or handling cybersecurity incidents often require immediate cross-border, cross-agency information sharing as cyberspace is not restricted to the physical world's boundaries. Such sensitive information sharing is only possible if the required legal framework, mutual trust and operative cooperation exist between the parties. The EU provides this trusted environment and facilitates cooperation: Europol, ENISA, CERT-EU and other EU agencies provide the central hub for information sharing between national agencies and entities. Police cooperation through Europol is an integral and operative part of handling cyber-related aspects of crime-fighting in both countries. Also, since the EU is also a regulatory power, either through soft or hard law, cybersecurity-related economic, JHA or other social policies can be coordinated and enforced between member states to extend further the values provided by the EU. This research found two pieces of evidence for that: the cybersecurity certification and legislation on cryptocurrencies. Cyber certification of goods entering the EU market found to be a relevant topic for the Netherlands, which argued for an EU level legislation. Both countries found that the anonymity and lack of traceability of fiscal

transactions leveraging cryptocurrencies possess new criminal threats, and both countries support EU level legislation on cryptocurrencies.

As for the external security aspects, both the Netherlands and Hungary – the latter, which often objects to joint CFSP statements – considers the EU's Cyber Diplomacy Toolbox an important tool in cybersecurity. They consider it a complement to NATO's cyber deterrence capabilities as economic sanctions as part of cybersecurity diplomatic actions leveraging the economic power of the whole EU provide effective countermeasures and deterrence against nation state-supported cyber attacks. They both argue that the most challenging aspect of the proper diplomatic response is attribution – gathering adequate evidence against and identifying a malicious actor – because the relevant information might be outside of the authority of a given state due to the cross-border nature of cyberspace. The trusted and operative environment provided by the EU helps states in this as well: it facilitates voluntary information sharing with 'Like-minded' states and the option for an effective joint diplomatic action through the Cyber Diplomacy Toolbox. The importance of cooperation with 'Like-minded' states also enhances the diplomatic weight of the countries in other international organizations, such as the CoE, OSCE or UN, and allows a better global cybersecurity presence.

The research also found evidence on the positive impacts of Europeanization and integration. The Netherlands aims to be a leader in cybersecurity legislation at the EU level due to the high level of digitalization of the country. Hungary benefits from the EU as the country can take best practices and directly benefits from EU-level legislation. The interdependence due to cooperation in other areas – most relevantly the single market – also makes it necessary for member states to coordinate their efforts in cybersecurity. Both states expect further digitalization – especially with the COVID pandemic, which contributed to an unprecedented rise in online activity – and new technologies, such as Artificial Intelligence and 5G, will further drive dependency on ICT. Both states consider the EU as a natural form for the necessary legislation on cyberspace. The NIS Directive was adopted in 2016, and the 'enhanced' NIS2 Directive is already under negotiation. Both Hungary and the Netherlands have high expectations for the new directive and expect to enhance cybersecurity further and improve cyber resilience. In case of Hungary, further evidence of Europeanization is that it operationalizes Eurostat data to determine the cyber resiliency of its society by comparing the country's readiness to other EU member states.

This research aimed to investigate the added value of the EU for Hungary and the Netherlands. These countries were selected as they both are members of NATO as well. However, further research should investigate the EU's added value to non-NATO member states. That would enable gaining further insights into the values provided by the EU, especially if comparing with the findings of this research. Also, the two cases were selected as medium-sized EU members, as the added value of EU for large member states – such as Germany or France – would be different due to their international diplomatic weight and economic importance. Similarly interesting would be to investigate the added value of smaller member states - such as Malta and Luxembourg – as their international dependency, especially in cyber, is even more pronounced than the two states included in this research. The key finding of this research is that since cybersecurity is cross-boundary by nature and covers multiple policy areas, it requires an environment that is trusted, operative, and legislative in nature, and the EU provides all these aspects. Thus, the EU became an integral part of ensuring its citizens' safety and security in cyberspace. Further research could also investigate what other areas that require such trusted, operative and legislative cooperation – such as handling the implications of a global pandemic – can learn from the achievements of the cybersecurity cooperation in the European Union.

Bibliography

Alexandra Brzozowski. 2021. ‘Germany Slams “Hostage-Taking” of EU’s Foreign Policy’. *Euractive* (Online). https://www.euractiv.com/section/global-europe/news/germany-slams-hostage-taking-of-eus-foreign-policy/ (June 19, 2021).

Alicia Parlapiano. 2016. ‘What We Know About the Cyberattack on Democratic Politicians?’ *The New York Times* Online(Online). https://www.nytimes.com/interactive/2016/08/16/us/politics/cyberattack-on-democratic-politicians-dnc.html.

Boeke, Sergei, Caitriona H. Heinl, and Matthijs A. Veenendaal. 2015. ‘Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices across Asia and Europe’. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, Tallinn, Estonia: IEEE, 69–80. http://ieeexplore.ieee.org/document/7158469/ (February 20, 2021).

Carrapico, Helena, and André Barrinha. 2017. ‘The EU as a Coherent (Cyber)Security Actor?: The EU as a Coherent (Cyber)Security Actor?’ *JCMS: Journal of Common Market Studies* 55(6). http://doi.wiley.com/10.1111/jcms.12575 (February 22, 2021).

Christou, George. 2016. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Palgrave.

———. 2018. ‘The Challenges of Cybercrime Governance in the European Union’. *European Politics and Society* 19(3). https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430722 (February 22, 2021).

———. 2019. ‘The Collective Securitisation of Cyberspace in the European Union’. *West European Politics* 42(2). https://www.tandfonline.com/doi/full/10.1080/01402382.2018.1510195 (February 22, 2021).

Cini, Michelle, and Angela K. Bourne, eds. 2006. *Palgrave Advances in European Union Studies*. Basingstoke [England] ; New York: Palgrave Macmillan.

Council of Europe. 2001. ‘Treaty No.185 - Convention on Cybercrime’. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (April 25, 2021).

Council of the European Union. 2017. *Draft Council Conclusions on a Framework or a Joint EU Diplomatic Response to Malicious Cyber Activities (‘Cyber Diplomacy Toolbox’) - Adoption*. Brussels: Council of the European Union. ‘I/A’ ITEM NOTE. https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf (March 14, 2021).

Couzigou, Irène. 2018. 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations'. *International Review of Law, Computers & Technology* 32(1). https://www.tandfonline.com/doi/full/10.1080/13600869.2018.1417763 (February 20, 2021).

Dennis Broeders, Els De Busser, and Patryk Pawlak. 2020. 'Three Tales of Attribution in Cyberspace Criminal Law, International Law and Policy Debates'. https://eucyberdirect.eu/wp-content/uploads/2020/04/three-tales-of-attribution-in-cyberspace.pdf (October 21, 2020).

Di Camillo, Federica, and Valérie Miranda. 2011. *Ambiguous Definitions in the Cyber Domain: Costs, Risks and the Way Forward*. Istituto Affari Internazionali (IAI).

Dunn Cavelty, Myriam. 2014. 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities'. *Science and Engineering Ethics* 20(3): 701–15.

Elkhannoubi, Hasna, and Mustapha Belaissaoui. 2015. 'A Framework for an Effective Cybersecurity Strategy Implementation: Fundamental Pillars Identification'. In *2015 15th International Conference on Intelligent Systems Design and Applications (ISDA)*, Marrakech, Morocco: IEEE, 1–6. http://ieeexplore.ieee.org/document/7489156/ (February 20, 2021).

European Commission. 2020a. 'Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Measures for a High Common Level of Cybersecurity across the Union, Repealing Directive (EU) 2016/1148'. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union (June 22, 2021).

———. 2020b. 'The EU's Cybersecurity Strategy for the Digital Decade'. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (June 22, 2021).

Foley, Paul et al. 2020. *International Digital Economy and Society Index 2020: final report.* https://op.europa.eu/publication/manifestation_identifier/PUB_KKBC20001ENN (June 6, 2021).

Fuchs, Thomas A. E. 2018. 'The Limits of European Integration Theories: Cyber-Development and the Future of the European Union'. In *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, eds. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos. Cham: Springer International Publishing, 113–37. http://link.springer.com/10.1007/978-3-319-09069-6_62 (February 22, 2021).

Gabi Siboni and David Siman-Tov. 2014. 'Cyberspace Extortion: North Korea versus the United States'. *The Institute for National Security Studies, Tel-Aviv University* (Online). https://www.inss.org.il/publication/cyberspace-extortion-north-korea-versus-the-united-states/ (June 23, 2021).

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge, Mass: MIT Press.

Government of Hungary (Magyarország Kormánya). 2012. 'Government decree 1035/2012. (II. 21.) on Hungary's national security strategy (A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról)'. https://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf (April 25, 2021).

———. 2013. 'Government decree 1139/2013. (III. 21.) on Hungary's national cyber-security strategy (A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról)'. https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf (April 25, 2021).

———. 2018. 'Government decree 1838/2018 (XII.28) Hungary's network and information systems security strategy (Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján)'. http://2015-2019.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse (April 25, 2021).

———. 2020. 'Government decree 1163/2020. (IV. 21.) on Hungary's national security strategy (1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról)'. https://nbsz.gov.hu/docs/NBS_MK_2020_81_1163.2020_Korm.hat.pdf (April 25, 2021).

High Representative of the European Union. 2013. 'EU Cyber Security Strategy: An Open, Safe and Secure Cyberspace'. https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en (April 25, 2021).

Irene Kamara, Ronald Leenes, Kees Stuurman, and Jasper van den Boom. 2020. 'The Cybersecurity Certification Landscape in the Netherlands after the Union Cybersecurity Act'. https://www.ncsc.nl/onderzoek/documenten/rapporten/2020/oktober/2/the-cybersecurity-certification-landscape-in-the-netherlands-after-the-union-cybersecurity-act (June 2, 2021).

Jensen, Eric Talbot. 2015. 'Cyber Sovereignty: The Way Ahead'. *Texas International Law Journal* 50(2-3): 275-304.

Kaiser, Robert. 2015. 'The Birth of Cyberwar'. *Political Geography* 46: 11–20.

Laurens Cerulus. 2021. 'EU to Launch Rapid Response Cybersecurity Team'. *Politico* (Online). https://www.politico.eu/article/eu-joint-cyber-unit-rapid-response-cyberattacks/ (June 23, 2021).

Lee Mathews. 2020. ‘Cyberattack On A Hospital Leads To The First Ransomware-Linked Death’. *Forbes* (Online). https://www.forbes.com/sites/leemathews/2020/09/17/ransomware-attack-hospital-leads-to-death/?sh=779b8be13f05 (June 23, 2021).

Lisa-Maria Neudert, Philip Howard, and Bence Kollanyi. 2019. ‘Sourcing and Automation of Political News and Information During Three European Elections’. *Social Media + Society* 5(3). http://journals.sagepub.com/doi/10.1177/2056305119863147 (June 23, 2021).

Loader, Ian. 2002. ‘Policing, Securitization and Democratization in Europe’. *Criminal Justice* 2(2). http://journals.sagepub.com/doi/10.1177/1748895802002020201 (June 12, 2021).

Magnette, Paul. 2005. *What Is the European Union? Nature and Prospects*. Houndmills, Basingstoke, Hampshire ; New York, N.Y: Palgrave Macmillan.

Majone, Giandomenico. 1998. ‘Europe’s “Democratic Deficit”: The Question of Standards’. *European Law Journal* 4(1). http://doi.wiley.com/10.1111/1468-0386.00040 (June 12, 2021).

———. 2005. *Dilemmas of European Integration: The Ambiguities and Pitfalls of Integration by Stealth*. Oxford ; New York: Oxford University Press.

Moravcsik, Andrew. 2002. ‘Reassessing Legitimacy in the European Union’. *JCMS: Journal of Common Market Studies* 40(4). http://doi.wiley.com/10.1111/1468-5965.00390 (June 12, 2021).

National Coordinator for Counterterrorism and Security (NCTV). 2019a. ‘Cybersecurity Agenda - Digital security of The Netherlands (Nederlandse Cybersecurity Agenda)’. https://www.nctv.nl/themas/cybersecurity/documenten/publicaties/2018/04/21/nederlandse-cybersecurity-agenda (June 9, 2021).

———. 2019b. ‘Integrated Risk Analysis, National Security (Geïntegreerde Risicoanalyse Nationale Veiligheid)’. https://www.nctv.nl/binaries/nctv/documenten/publicaties/2019/6/07/geintegreerde-risicoanalyse-nationale-veiligheid/TK-bijlage-geintegreerde-risico-analyse-nationale-veiligheid_tcm31-393838.pdf (February 5, 2021).

———. 2019c. ‘National Security Strategy 2019 (Nationale Veiligheid Strategie 2019)’. https://www.nctv.nl/binaries/nctv/documenten/publicaties/2019/6/07/nationale-veiligheid-strategie-2019/Nationale+Veiligheid+Strategie+2019.pdf (February 5, 2021).

———. 2020. ‘Cybersecurity Landscape of The Netherlands (Cybersecuritybeeld Nederland)’. https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland/documenten/publicaties/2020/06/29/cybersecuritybeeld-nederland-2020 (February 5, 2021).

———. 2021. ‘Mid-term evaluation of the Natonal Security Strategy 2019 (Tussentijdse evaluatie Nationale Veiligheid Strategie 2019)’. https://www.nctv.nl/binaries/nctv/documenten/rapporten/2021/03/08/tussentijdse-

evaluatie-nationale-veiligheid-strategie-2019/Tussentijdse+evaluatie+Nationale+Veiligheid+Strategie+2019.pdf (February 5, 2021).

National Cyber Security Centre (NCSC). 2020. 'National Crisis plan – Digital (Nationaal Crisisplan Digitaal)'. https://www.ncsc.nl/documenten/publicaties/2020/februari/21/nationaal-crisisplan-digitaal (June 9, 2021).

National Health Institution, Ministry of Health, Wellbeing and Sport. 2020. 'National Security Horizon Scan 2020 (Horizonscan Nationale Veiligheid (2020))'. https://www.rivm.nl/documenten/horizonscan-nationale-veiligheid-2020 (June 13, 2021).

North Atlantic Treaty Organization. 2020. 'Cyber Defence'. https://www.nato.int/cps/en/natohq/topics_78170.htm (October 22, 2020).

Odermatt, Jed. 2018. 'The European Union as a Cybersecurity Actor'. In *Research Handbook on the EU's Common Foreign and Security Policy*, Research handbooks in European law, eds. Panos Koutrakos and Steven Blockmans. Cheltenham, UK: Edward Elgar Publishing.

Olsen, Johan P. 2002. 'The Many Faces of Europeanization'. *JCMS: Journal of Common Market Studies* 40(5). http://doi.wiley.com/10.1111/1468-5965.00403 (June 12, 2021).

Piret Pernik. 2014. *Improving Cyber Security: NATO and the EU*. Tallinn: International Centre for Defence Studies. Analysis. https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf (February 22, 2021).

Samonek, Aleksandra. 2020. 'What Is the Future of European Cyber Security? Three Principles of European Cooperation and the Hybrid Joint Strategy of Cyber Defence'. *Studia Europejskie - Studies in European Affairs* 24(2): 43–60.

Scharpf, Fritz Wilhelm. 1999. *Governing in Europe: Effective and Democratic?* Oxford ; New York: Oxford University Press.

Simon Hix. 2008. 'What's Wrong with the European Union and How to Fix It'. *Ethics & International Affairs* 23(3). https://www.cambridge.org/core/product/identifier/S0892679400006432/type/journal_article (June 12, 2021).

Sliwinski, Krzysztof Feliks. 2014. 'Moving beyond the European Union's Weakness as a Cyber-Security Agent'. *Contemporary Security Policy* 35(3): 468–86.

Tikk, Eneken, and Mika Kerttunen, eds. 2020. *Routledge Handbook of International Cybersecurity*. New York: Routledge, Taylor & Francis Group.

Tomic, Dusko, Eldar Saljic, and Danilo Cupic. 2018. 'Cyber-Security Policies of East European Countries'. In *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*, eds. Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos.

Cham: Springer International Publishing, 1039–55. http://link.springer.com/10.1007/978-3-319-09069-6_59 (February 22, 2021).

Weiler, J.H.H. 1995. 'Does Europe Need a Constitution? Demos, Telos and the German Maastricht Decision'. *European Law Journal* 1(3). http://doi.wiley.com/10.1111/j.1468-0386.1995.tb00030.x (June 12, 2021).

Wille, A. C. 2013. *The Normalization of the European Commission: Politics and Bureaucracy in the EU Executive*. Oxford: Oxford University Press.

Zimmermann, Hubert, and Andreas Dür, eds. 2016. *Key Controversies in European Integration*. 2nd edition. London New York: Macmillan Education, Palgrave.