MASTERARBEIT | MASTER'S THESIS

Titel | Title

The Role of Member States in Influencing the EU Cyber Diplomacy Toolbox: A Europeanisation Perspective

verfasst von | submitted by

David Henri Joseph Mentz BA

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt | Degree programme code as it appears on the student record sheet:	UA 066 824
Studienrichtung lt. Studienblatt | Degree programme as it appears on the student record sheet:	Masterstudium Politikwissenschaft
Betreut von | Supervisor:	ao. Univ.-Prof. Mag. Dr. Gerda Falkner

Abstract

(EN) While the EU's Cyber Diplomacy Toolbox has generally been welcomed, it has also been a point of contention between member states. This thesis aims to contribute to the existing body of research on using diplomatic tools to achieve cybersecurity objectives by examining its development from the perspective of member states, which can help to understand how member states behave about the Europeanisation of CFSP. The literature so far has looked mainly at the toolbox application but has not yet zoomed in at its development from a member state perspective. To answer the question "*How have EU member states influenced the development of the EU Cyber Diplomacy Toolbox*?"*,* a qualitative text analysis of statements from news (Agence Europe and Euractiv) and EU sources (the Council) between 2017 and 2025 has been conducted. This identified national preferences, which were coded according to 'uploading', 'cross-loading', 'spillover', 'autonomy' and 'Europeanisation'. The study finds that, while Europeanisation prevails overall, sovereignty-oriented standpoints are also evoked, surprisingly occasionally also by member states that generally position themselves as Europeanisers. Member states actively voice their national priorities at the EU level to achieve their desired outcomes, but they also seek to avoid difficult issues when they arise. Finally, the findings are interpreted in light of the theories of Europeanisation: intergovernmentalism, neofunctionalism and postfunctionalism, to provide an interpretation for some of the observations.

(DE) Die *Cyber Diplomacy Toolbox* der EU wurde zwar allgemein von den Mitgliedsstaaten begrüßt, war jedoch auch Gegenstand von Diskussionen. Diese Arbeit soll einen Beitrag zur bestehenden Forschung über den Einsatz diplomatischer Instrumente zur Erreichung von Cybersicherheitszielen leisten, indem sie die Entwicklung der *Cyber Diplomacy Toolbox* aus der Perspektive der Mitgliedstaaten untersucht, um das Verhalten der Mitgliedstaaten hinsichtlich der Europäisierung der GASP zu verstehen. Die bisherige Literatur hat sich hauptsächlich mit der Anwendung der Toolbox befasst, aber noch nicht die Entwicklung aus der Perspektive der Mitgliedstaaten beleuchtet. Um die Frage „Wie haben die EU-Mitgliedstaaten die Entwicklung der EU *Cyber Diplomacy Toolbox* beeinflusst?" zu beantworten, wurde eine qualitative Textanalyse von Aussagen aus Nachrichten (Agence Europe und Euractiv) und EU-Quellen (Ratsdokumente) zwischen 2017 und 2025 durchgeführt. Dabei wurden nationale Präferenzen identifiziert, die nach den Kriterien „Uploading", „Cross-Loading", „Spillover", „Autonomie" und „Europäisierung" kodiert

wurden. Die Arbeit kommt zu dem Ergebnis, dass zwar insgesamt Europäisierung überwiegt, aber auch souveränitätsorientierte Standpunkte zum Ausdruck kommen, überraschenderweise gelegentlich auch von Mitgliedstaaten, die sich im Allgemeinen als Europäisierer positionieren. Die Mitgliedstaaten bringen ihre nationalen Prioritäten auf EU-Ebene aktiv zum Ausdruck, um ihre gewünschten Ergebnisse zu erzielen, versuchen aber auch, schwierige Themen zu vermeiden, wenn sie auftauchen. Schließlich werden die Ergebnisse im Lichte der Theorien zur Europäisierung interpretiert: Intergouvernementalismus, Neofunktionalismus und Postfunktionalismus, um eine Einordnung für die Beobachtungen zu liefern.

Abstract 1

1. Introduction 6

What Is the Cyber Diplomacy Toolbox 7

Who is responsible for Cyber diplomacy within the EU 8

The development of the Cyber Diplomacy Toolbox 9

The 2015 conclusions on Cyber Diplomacy 9

2017 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities 10

Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796 11

2023 Revised Implementing Guidelines of the Cyber Diplomacy Toolbox 13

Strategy papers and Conclusions 14

Relevance and Research gap 14

Research approach 15

2. Literature review 17

What is cyber diplomacy in the literature? 17

The application of the Cyber Diplomacy Toolbox 18

The EU's Influence in Global Cyber Security and international law in cyberspace 19

The EU and NATO in cyber diplomacy 20

The Issues of attribution 21

Can effective cyber deterrence exist without hard power? 23

3. Theoretical Framework 24

Europeanisation-Autonomy 25

Classical Europeanisation Theories 26

Postfunctionalism 26

Intergovernmentalism 27

Neofunctionalism 28

Spillovers 29

Ramifications for the Cyber Diplomacy Toolbox Development 31

Uploading and Cross-loading 31

Uploading 32

Cross-loading 34

4. Methodology 36

Research Design 36

Data Collection and Corpus 37

Coding operationalisation 39

Coding Process 40

Dealing with track changes 40

Defining the field of cyber diplomacy in contrast to cybersecurity and hybrid threats. 41

5. Comparative Patterns of Europeanisation and Autonomy 42

Example 2: there are five 'Yes' values for Estonia concerning the 'Europeanisation' code for a statement made by Estonia alone. As there are 18 additional statements made by Estonia with other member states that have this code, the numbers of 'Yes' with and without brackets are 5 (23). 43

Tacit acceptance 43

Application of the toolbox as an expression of Europeanisation. 44

On the 2018 and 2020 non-papers 45

By Country 47

Austria 47

Belgium 48

Bulgaria....49
Czechia....49
Denmark....50
Estonia....51
Finland....52
France....53
Germany....55
Greece....58
Hungary....58
Ireland....60
Italy....62
Latvia....64
Lithuania....65
Malta....66
Netherlands....66
Poland....70
Portugal....71
Romania....72
Slovakia....72
Slovenia....74
Spain....74
Sweden....74
UK....76
Comparison of findings....79

Postfunctionalism....82
Intergovernmentalism....83
Neofunctionalism....85
Europeanisation of Foreign Policy....86
Considering the research questions....87
How have EU member states influenced the development of the EU Cyber Diplomacy Toolbox?....87
Do governments attempt to upload or cross-load national preferences in their statements?....89
Which governments support or oppose transferring competences to the EU, and do their documented positions reveal spillover tendencies?....89
Link to the literature....91
6. Conclusion....93
What have we found....93
Theoretical and practical takeaways....94
Future research and limitations....95
7. Sources....96
Abbreviations and Software....104

1. Introduction

For EU member states, cybersecurity has become a critical domain for national defence and sovereignty. States have recognized this and are increasingly leveraging diplomatic channels and coordination with partners to amplify their voices and achieve their security goals. By actively engaging in EU frameworks, states can influence collective cyber norms and standards, thereby exerting greater influence.

In this context, the EU Cyber Diplomacy Toolbox, launched in 2017, is the EU's primary tool within the Common Foreign and Security Policy for engaging in cyber diplomacy with third parties. It includes a range of measures aimed at enhancing cybersecurity within the EU and influencing the behaviour of foreign governments in cyberspace to align with EU norms. After successive cyber-incidents, the Council has repeatedly utilized the toolbox's capabilities to sanction persistent threat actors (see Council, 2025). Over time, the toolbox has evolved and now includes multiple implementing guidelines, regulations, decisions, and notes. This progress has been largely driven by the advocacy of certain member states (see Ivan, 2019, p. 7) aiming to shift the sanctions regime towards more tangible actions.

What Is the Cyber Diplomacy Toolbox

The Cyber Diplomacy Toolbox comprises measures to be implemented within the EU Common Foreign and Security Policy to engage in cyber diplomacy with third parties. It was launched in 2017, reinforced in 2019, and first employed in 2020 (Kasper et al., 2021, p. 9).

The Cyber Diplomacy Toolbox is commonly separated into five types of actions (Ivan, 2019, p. 5):

1. Preventive measures (EU-supported confidence-building measures, raising awareness of EU policies and EU cyber capacity building in third countries (Latici, 2020, p. 8)). Preventive measures consist of less intrusive means that aim to prevent cyber conflict from emerging in the first place, thus serving as the first line of defence. (Alatalu & Austin, 2020, p. 5).

2. Cooperative measures (cooperation through EU-led political and thematic dialogues or through démarches by EU delegations (Latici, 2020, p. 8)). Cooperative measures seek a joint response to an emerging situation by engaging other international organisations and third countries (Sachs et al., 2024, p. 5).

3. Stability measures (statements by the High Representative and on behalf of the Council of the EU, EU Council conclusions, diplomatic démarches by EU delegations (Latici, 2020, p. 8) and signalling through EU-led political and thematic dialogues (Moret et al., 2017, p. 4). Stability measures consist of diplomatic initiatives that aim to signal the EU's stance on certain issues and warn of further consequences if undesirable behaviour continues (Kasper et al., 2021, p. 8). In this context, Council conclusions serve to encourage member states to take

further action, while making direct attribution by the EU itself unnecessary (Sachs et al., 2024, p. 5).

4. Restrictive measures. Restrictive measures are the most escalatory yet also, the most tangible instruments available to the EU in response to malevolent cyber activities. These actions are based on Articles 29 of the Treaty on European Union (TEU) and 215 of the Treaty on the Functioning of the European Union (TFEU) (Council, 2017(2), p. 9). In theory, they could be used to sanction organisations, individual actors but also provide for the sanctioning of entire governments (Poli & Sommario, 2023, p. 524); however, thus far, no countries have been sanctioned under these measures. Most sanctioned entities are associated with government-sponsored persistent threat actors. The current list of sanctioned entities can be found in Annex I of Council Regulation (EU) 2019/796 of 17 May 2019. As of writing, the list includes 18 entries: Four groups or legal persons and fourteen associated physical persons (Council, 2025). Sanctions consist of travel bans and the seizure of financial assets (Sachs et al., 2024, p. 6).

5. Possible EU support to Member States' lawful responses (Council, 2017(2), pp. 6-10) (Auswärtiges Amt, 2020, p. 7). Lawful responses are instances in which individual member states are taking measures to counter serious malevolent cyber activities and are supported by the EU through various mutual assistance and solidarity mechanisms under Art. 222 TFEU and the mutual defence clause of Article 42(7) TEU (Latici, 2020, p. 8). Referencing these two articles underlines the severity of the cyber action required to trigger these mechanisms, as both articles refer to significant physical attacks such as armed aggression, catastrophes, or terrorist attacks (see European Union, 2008, Article 42 TEU) (European Union, 2016, Article 222 TFEU). So far, these articles have not been triggered as part of the Cyber Diplomacy Toolbox (Sachs et al., 2024, p. 6)**.**

Who is responsible for Cyber diplomacy within the EU

Member states retain the primary role in cyber diplomacy, with the EU assuming a 'supportive, coordinative and advisory' role (Kasper & Vernygora, 2021, p. 34) Within the Council, the 'Horizontal Working Party on Cyber Issues' deals with most cyber diplomacy matters (Bendiek, 2018, p. 3). The EEAS also has a cyber diplomacy team; civilian information matters are handled by the EU INTCEN, while the military side is managed by the EUMS INT (Bendiek, 2018, p. 3).

Member states remain the main actors in CFSP. However, they also see their foreign policies as integrated into European CFSP. This is done by justifying their position at the European level (see Wong and Hill, 2011, p. 17). They still have their own foreign policy apparatuses, goals, diplomats, and the ability to enhance their reach through the EU, while at the same time consulting in the Council and working groups.

The development of the Cyber Diplomacy Toolbox

Sara Poli and Emanuele Sommario (2023, pp. 532-533) argue that the EU has only recently emerged as a cybersecurity actor for member states. Agnes Kasper and Vlad Vernygora (2021, p. 35) and Paul Ivan (2019, p. 5) set the start-date of the toolbox's development in 2016 with the Dutch presidency of the Council and the non-paper on a joint EU-deterrence mechanism for cybersecurity. The 2016 Council proposal for a joint EU response to malicious cyber-actions led to the toolbox being finalised in 2017.

The 2015 conclusions on Cyber Diplomacy

Prior to this, the Council had already published the *'2015 Conclusions on Cyber Diplomacy'* and the *'2013 EU Cybersecurity Strategy'*, which laid the groundwork for the toolbox (Kasper & Vernygora, 2021, p. 57). At that point, cyber sanctions were a novel concept, having first been used by the Obama administration in 2015 (Bendiek, 2018, p. 5).

The *'2015 Conclusions on Cyber Diplomacy'* focuses more on issues related to cybercrime and cyberterrorism, it already outlines many of the values found in later texts, even though it does not mention the possibility of cyber sanctions or address issues stemming from state-controlled malevolent actors. The text emphasises the importance of upholding human rights, free speech and EU values online (Council, 2015, pp. 3-4). It establishes a number of guiding principles that can be found in later cyber diplomacy acts, such as private-public cooperation (Council, 2015, p. 4), capacity building in third countries (Council, 2015, pp. 4-5), freedom of expression and information (Council, 2015, p. 4), the rule of international law in cyberspace, and respect for the work of international organisations (Council, 2015, p. 11)(Council, 2015, pp. 5-6). The text stipulates that member states should ensure that capacity building promotes EU values and conduct in cyberspace (Council 2015, p. 9), which is also evident in Annika Sachs, Imke Schmalfeldt and Kerstin Zettl-Schabath's analysis of the toolbox's application (Sachs et al., 2024, pp. 16-17). The text also notes the importance of empowering women and girls (Council,

2015, p. 5). It pays particular attention to the importance of digital technologies and data, the single market, and economic competitiveness and prosperity (Council, 2015, pp. 8-9).

Notably, the Council Conclusions emphasise that they do not affect the distribution of competencies between the member states and the EU. They also explicitly mention the principle of subsidiarity (see Council, 2015, p. 5). In this context, the conclusions state that the EU and its member states should uphold the principles of responsible state behaviour in cyberspace (Council, 2015, p. 7). At the same time, however, it does call for greater collaboration between member states and the EU regarding sharing information and expertise (Council, 2015, p. 12), as well as increased coherence in national policies and initiatives (Council, 2015, p. 12).

2017 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities

The toolbox was developed under the 2017 Estonian 'digital presidency' (Alatalu & Austin, 2020, p. 180) as part of the Cybersecurity Package. It bridges the CFSP and national member states interests in Cyber and Cyber Defence and develops a collective cyber deterrence and signalling regime that includes sanctions (Alatalu & Austin, 2020, pp. 180-18). The *2017 Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* acknowledge the increased malicious activities by both state and non-state actors. To this end, the EU emphasises that malicious cyber activities can constitute internationally wrongful acts, or at least cybercrimes (Council, 2017(1), p. 3). In this context, the toolbox is intended to prevent attacks by acting as a deterrent (Council, 2017(1), p. 4). While it does not yet establish a framework for a joint EU diplomatic response, it does set out a number of main principles to guide the framework, including respect for international law and human rights, agreement by member states, proportionality and the attainment of CFSP objectives, as well as the protection of the security of the EU and its member states (Council, 2017(1), p. 4).

The 2017 guidelines explain the toolbox's role in dealing with hybrid threats to the EU. It is a supportive framework that works alongside other mechanisms such as the UN Charter, the *Budapest Convention on Cybercrime* and the work of the *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications*

in the Context of International Security. The Toolbox is not intended to replace the actions of individual member states or groups of member states in response to cyberattacks, and member states retain their right to conduct their own foreign policy. The guidelines explicitly mention the possibility of a state carrying out malicious cyber activity directly (Council, 2017(2), p. 5) or allowing such activity to be carried out from its territory without taking action to stop it (Council, 2017(2), p. 5).

The framework can be applied either through the Integrated Political Crisis Response mechanism agreed by the Council (2017(2), p. 10), or through the mechanism provided for in the guidelines. This involves sharing information and situational awareness between member states and the EU to create a mutual understanding of the threat. This can be coordinated by EUIBAS, such as the EU Intelligence and Situation Centre, the CSIRTs network, the EC3, ENISA or CERT-EU (Council, 2017(2), p. 11), or by the Council's Horizontal Working Party on Cyber Issues and the Political and Security Committee when considering the application of the toolbox (Council, 2017(2), p. 12). Member states, the EEAS and the High Representative may submit an initiative for the application of the toolbox to the Council (Council 2017(2), p. 12). While attribution remains the sovereign right of member states (Council, 2017(2), p. 13), Intcen, supported by EUIBAS (e.g. CERT-EU or ENISA), can assist with the attribution of cyberattacks (Council, 2017(2), p. 13). The Horizontal Working Party on Cyber Issues serves as the preparatory committee for all toolbox applications. It is consulted by the Foreign Relations Counsellors Working Party and the Political and Security Committee. (Council, 2017(2), p. 15).

Council Decision (CFSP) 2019/797 and Council Regulation (EU) 2019/796

The Joint Communication of the European Parliament, the Council and the European Council, entitled *'Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats'* and published on 13 June 2018, called for the toolbox to be used more often by member states, as this would increase its effectiveness over time (European Commission 2018 p. 8). It also called for member states to work towards a common attribution scheme and increased intelligence sharing (European Commission 2018 p. 9).

In 2019, the toolbox was enhanced by the introduction of specific legislation in the form of *Council Decision (CFSP) 2019/797* and *Council Regulation (EU) 2019/796* (Sachs et al., 2024,

p. 6), creating a more robust cyber-sanctions regime. Council Regulation (EU) 2019/796 provides the first concrete definition of the scope of the sanctions regime in response to data or ICT system access or interference stemming from outside the Union, involving the use of Union infrastructure, or carried out directly from outside the Union by legal or physical persons, entities, or bodies (Council 2019(1), p. 2). The relevant targets of cyber-attacks that might trigger the regulation include member states, infrastructure, satellites, undersea cables and services that provide critical functions to the state or individuals, such as energy and transport. They also include the storage of classified information and government emergency response teams (Council, 2019(1), pp. 2-3). The EU may invoke the regime when institutions, bodies, offices, agencies and delegations, or CFSP operations, are targeted (Council, 2019(1), p. 3), or when it is deemed necessary for CFSP goals, for example when attacks target third countries (Council 2019(1), p. 3).

The crux of the cyber sanctions regime can be found on page five, in Article 3: *'All funds and economic resources belonging to, owned, held or controlled by any natural or legal person, entity or body listed in Annex I shall be frozen'* (Council, 2019(1), p. 5). The rest of the document outlines the specifics of the sanctions regime and the conditions under which funds can be released (Council, 2019(1), p. 6) and explains how the list of sanctioned entities should be compiled in Annex I of the document (Council, 2019(1), p. 9).

Council Decision (CFSP) 2019/797 outlines some of the intentions of the toolbox, such as clearly signalling consequences to potential aggressors to serve as a deterrent and to achieve the CFSP objectives outlined in Article 21 TEU, but also clearly stating that attribution rests with each individual member state. The decision reiterates the legislation regarding economic sanctions (Council, 2019(2), pp. 4-5) and establishes provisions for denying entry to the EU in Article 4: *'Member States shall take the measures necessary to prevent the entry into, or transit through, their territories of: (a)natural persons who are responsible for cyber-attacks or attempted cyber-attacks; (b) natural persons who provide'...' support for or are otherwise involved in cyber-attacks'...' (c) natural persons associated with the persons covered by points (a) and (b)'* (Council, 2019(2) p. 3). Furthermore, Article 6 outlines the rules for establishing the list of sanctioned entities: '*The Council, acting by unanimity upon a proposal from a Member State or from the High Representative of the Union for Foreign Affairs and Security*

Policy, shall establish and amend the list set out in the Annex' (Council, 2019(2), p. 5). The decision was amended in 2023 and is valid until 18 May 2025 (Council, 2023(1), p. 1).

2023 Revised Implementing Guidelines of the Cyber Diplomacy Toolbox

In 2023 the toolbox was updated with the *Revised Implementing Guidelines of the Cyber Diplomacy Toolbox* (Council 2023 (2) p. 1). The document states that the EU must do more to deter malicious cyberactivities, calling for a coordinated EU response in the field of Cyber CFSP (Council 2023 (2), pp. 2-3). Strategic response notes are introduced. Response notes entail risk assessments for specific geographic scenarios or persistent threat actors (Council 2023 (2), p. 11). The issue of joint situational awareness and information sharing is given its own section which reaffirms that information sharing is voluntary, but crucial. The text attributes roles to newly created EU bodies, such as EU-CyCLONe (Council, 2023 (2), p. 13) and includes new legal developments, such as the updated EU Cybersecurity Crisis Response Framework (Council, 2023 (2), p. 14). The document outlines a step-by-step procedure for applying the toolbox (Council, 2023 (2), pp. 15-18) and highlights several considerations for attribution (Council, 2023(2), p. 19). The updated guidelines also foresee further cooperation with NATO, academia, and the private sector (Council, 2023(2), pp. 25-26), as well as the use of the toolbox to combat hybrid threats alongside the Hybrid Toolbox (Council, 2023(2), p. 22). Overall, the updated guidelines clarify many of the vague terms and frameworks present in the original guidelines by outlining concrete steps to determine attribution and providing a step-by-step mechanism for deliberating the application of the toolbox. They also define clearer mandates for the new EU cyber-adjacent bodies created in recent years.

The key takeaways from the documents described above are that, while unanimity in the Council remains a key requirement for implementing the measures described in the Cyber Diplomacy Toolbox, both the EU and its member states can initiate the process of applying the toolbox (Council, 2019(2), p. 5). Over time, the actions of the toolbox have become more tangible and the application process more streamlined. Issues of information sharing among member states and the common attribution of cyberattacks remain key obstacles to the successful application of the toolbox. Overall, the texts emphasise member states' sovereign right to attribute and apply the toolbox, while also suggesting that joint action would be more effective in achieving deterrence.

Strategy papers and Conclusions

In addition to the above-mentioned main texts relating to the Cyber Diplomacy Toolbox, we also have several strategy papers dealing with the broader topic of cybersecurity and cyber defence in the EU. Such as *The EU's Cybersecurity Strategy for the Digital Decade* of 2020, the 2021 *Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade*, the 2022 *Council conclusions on the development of the European Union's cyber posture*, the 2022 *EU Policy on Cyber Defence,* the 2022 *Council Conclusions on EU Digital Diplomacy* and the 2023 *Council Conclusions on the EU Policy on Cyber Defence.* All these documents mention the Cyber Diplomacy Toolbox in the context of the EU's cyber defence and cyber security strategy.

The 2020 Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, is particularly noteworthy. It includes the sentence that *'In addition, together with the Council and the Commission, the High Representative aims to consider additional measures under the cyber diplomacy toolbox, including further options for restrictive measures, as well as exploring qualified majority voting (QMV) for listings under the horizontal sanctions regime against cyber-attacks'* (European Commission, 2020, p. 17) instead of adhering to the agreed principle of unanimity within the Council. This shows that there is a divergence of ideas between sovereigntist and Europeanist forces on this topic.

Relevance and Research gap

Personally, I was interested in the Cyber Diplomacy Toolbox because I wanted to examine the concept of cyber deterrence by non-cyber means available to member states with limited cyber retaliation capabilities in order to mitigate potential threats. This has led me to take a closer look at the concept of common cyber deterrence via the Cyber Diplomacy Toolbox and how it has developed. Previous research on the Cyber Diplomacy Toolbox has primarily focused on how the EU uses it. However, not much research has yet considered the involvement of member states in shaping the toolbox itself. Member state governments play a significant role in shaping EU policy, particularly at the intersection of high politics and cyber governance, where governments, their representatives, diplomatic staff and experts notably influence common EU policy. While the literature has examined cases in which the toolbox was applied, and the

difficulties it faces in its application (see for example Sachs et al., 2024) or analysed the EU's approach to cyber diplomacy (see for example Kasper et al., 2021) so far little has been written about the development of the toolbox from a Europeanisation perspective.

The aim is to contribute to this field by investigating the toolbox's negotiation and which actors notably shaped it, explicitly following the gap in the literature mentioned by Ben Tonra (2015, p. 192) who suggested future research to take a closer look at member states attempting to fulfill their national interests in CFSP. Additionally, my theoretical and methodological approaches are novel in the context of the Cyber Diplomacy Toolbox. Thus far, the toolbox has not been examined through the lens of Europeanisation theories, nor has it been considered in terms of uploading and cross-loading. I hope that this will help us to better understand the impact of member states on policy in this field and what future cooperation in CFSP could entail.

The gap in the literature that is explored is the need to study how member states diverge on policy consensus (Tonra, 2015, p. 192), which is related to the Cyber Diplomacy Toolbox. Depending on their national preferences, member states may diverge significantly on the policies they wish to enact. This gap will be addressed by examining member state divergence in Europeanisation processes, and how member states attempt to influence CFSP policies as exemplified by the Cyber Diplomacy Toolbox.

Research approach

This work is based on the Europeanisation of foreign policy theories exemplified by Wong and Hill, and Tonra, to look at uploading and cross-loading in CFSP. On the other hand, classical Europeanisation theories will also be looked at to help explain the findings.

Member states seek to upload their policy preferences to the EU agenda (Bulmer and Lequesne, 2020, p. 5) by either using their own policy preferences as an example or pursuing their own goals based on other member states policies, policy suggestions and information. This is known as 'uploading' and 'cross-loading' (Tonra, 2015, p. 184), respectively. I opt for a broad definition of 'uploading', whereby 'uploading' consists of preference formulation regarding policy at the EU level in line with national priorities. 'Cross-loading' is then defined as the informal process of information exchange between member states on policy matters. Member states may view their foreign policy preferences threatened by this process and wish to maintain national

primacy. Alternatively, they may wish to ensure a functional Cyber Diplomacy Toolbox to mitigate the threats they face as well as support more EU-level competencies. Member states may seek to legitimise their respective policy preferences by referring to EU-level policies in other fields to justify their advocacy for more EU activities and powers in the field of cyber diplomacy; this is what I would describe as spillover.

According to the literature by Reuben Wong and Christopher Hill (2011), smaller member states are expected to adapt to EU positions, and post-neutral states are expected to revise their priorities based on common EU standpoints (Wong & Hill, 2011, p. 7). Larger member states play a major role in negotiating the CFSP (Wong & Hill, 2011, p. 10). This has also forced smaller states to expand their foreign policies to new fields, such as cyber diplomacy, as they have little chance of playing a major role in the international arena by acting unilaterally. They are therefore incentivised to act together with the larger member states or specialise themselves in niche fields. According to Paul Ivan (2019, p. 8), certain states have had success in promoting the Cyber Diplomacy Toolbox.

The concrete research question is *How have EU member states influenced the development of the EU Cyber Diplomacy Toolbox?*

Which I will attempt to answer using the sub-questions *Do governments attempt to upload or cross-load national preferences in their statements?* and *Which governments support or oppose transferring competences to the EU, and do their documented positions reveal spillover tendencies?*

The corpus was compiled from EU institutional websites (the Council, EUR-Lex and the European Commission) and supplemented with media sources such as Agence Europe and Euractiv. References to 'non-papers', which are documents not available in the Council archives, but which functioned as statements made at Council level, were also considered. Examples include non-papers available on the website of a participating state's Ministry of Foreign Affairs, or the priorities of a member state's Council presidency, provided they were referenced at Council level or by news sources. Keyword searches were used to identify relevant documents. The analysis covers the period from 2017 to May 2025, including the period following the official adoption and development of the toolbox.

The research relies primarily on a qualitative content analysis of both primary sources and secondary literature. The work follows Udo Kuckartz's (2014, p. 63) approach of deductive category construction: the categories are derived from the theories and the literature.

This was done using two axes: 'reasoning pattern' (uploading and cross-loading), as well as 'common response' (autonomy-Europeanisation). A code was also used for potential spillover. The idea is that using this coding method will enable identification of the stances of member states regarding the Cyber Diplomacy Toolbox.

2. Literature review

What is cyber diplomacy in the literature?

The literature on the CFSP is extensive and covers a wide range of topics. One recurring theme of interest to researchers is the potential for further alignment among member States. Cyber diplomacy is regarded as a distinct subfield within CFSP studies, situated at the intersection of cybersecurity and foreign policy practice. Amel Attafa, Karen Renaud and Stefano De Paoli (2020) distinguish cyber diplomacy from regular diplomacy when: *'the cyber dimension is the core reason for the diplomacy, it is cyber diplomacy'* (Attafa et al., 2020, p. 61). This contrasts with digital diplomacy, which refers to traditional diplomacy conducted using digital tools (Attafa et al., 2020, p. 61). In EU correspondence, particularly from the time when these terms first emerged, we find that they are sometimes used incorrectly or interchangeably by actors. Cyber diplomacy has emerged as its own field (Riordan, 2019, p. 3). Agnes Kasper, Anna Molnár and Anna-Maria Osula (2021) define cyber diplomacy as a field that addresses issues such as *'cybersecurity, cybergenic, cybercrime, confidence building, internet freedom and internet governance'*, and is carried out by diplomats (Kasper et al., 2021, p. 4). This distinguishes cyberdiplomatic activity from efforts led by non-traditional state actors or NGOs operating in cyberspace.

The following definition of cyber diplomacy is used in this paper: *Cyber diplomacy is the pursuit of cybersecurity objectives through foreign policy means*. Although they have significant shared objectives, cybersecurity and cyber diplomacy are different fields. While cybersecurity focuses on technical solutions and regulations to protect information systems and is primarily aimed at domestic actors, cyber diplomacy uses the measures in the Cyber Diplomacy Toolbox to target third states and their citizens.

The application of the Cyber Diplomacy Toolbox

One of the issues identified by Poli and Sommario is that it remains vague when to qualify cyberattacks as breaches of international law (2023, p. 526), and thus apply mechanisms of the toolbox, as acts should not trigger the restrictive measures of the toolbox when they are not emitted by states but rather fall under the category of cybercrimes.

Sachs, Schmalfeldt and Zettl-Schabath (2024) have systematically analysed the concrete application of the toolbox (2024, p. 6). They have found that over time, especially after the onset of Russia's war against Ukraine, the use of the toolbox has increased (Sachs et al., 2024, p. 21), of a total of 243 measures recorded by them, 58 were related to Ukraine (Sachs et al., 2024, p. 10). In total terms, Sachs and colleagues have found that preventive measures represent by far the largest share of actions taken with 105 from 2017 until 2023 (Sachs et al 2024 p. 9). The residual is made up of 63 cooperative measures and 73 stabilising measures (Sachs et al., 2024, p. 9). In the timeframe analysed, merely 2 restrictive measures were taken and no EU support for member states lawful responses was undertaken (Sachs et al., 2024, p. 9).

This is related to the issue of attribution (Sachs et al., 2024 p. 13) as it is easier to find consensus avoiding this issue of attribution by preferring to use the tools from the toolbox that do not require it (see Sachs et al., 2024, p. 13). Capacity building is mainly undertaken in states bordering Russia (Sachs et al., 2024, p. 14) and frequently related to bringing states cybersecurity up to EU standards or ensuring adherence to EU norms and values (Sachs et al., 2024, p. 16-17), such as by ensuring NIS-2 compatibility (Sachs et al., 2024, p. 15). At the same time, Sachs and colleagues find that France pursues its own capacity building initiatives on a bilateral basis with states, potentially seeking more influence in the affected countries (Sachs et al., 2024, p. 15).

Sachs and colleagues have also found that, the toolbox is more likely to be used when a state becomes a victim of a cyberattack, that holds considerable weight in the application of the toolbox, exemplified by the SolarWinds case, where the toolbox was implemented and the attack was attributed only after Germany got involved but not when Poland alone petitioned for the use of the toolbox or when Ireland was affected (Sachs et al., 2024, p. 18). Sachs and colleagues find that: *'the European Union appears to implement more robust measures only if a cyber incident affects another EU Member State that is particularly actively engaged in cyber*

diplomacy' (Sachs et al., 2024, p. 18). This serves as an important example of how the toolbox matters for member states and effective cyber diplomacy, as proponents have a higher chance of achieving coordinated action (Sachs et al., 2024, p. 21). Sachs and colleagues also find that during the beginning of Russia's war against Ukraine; effective use of the toolbox usage was possible as there was a coordinated effort among member states to support Ukraine (Sachs et al., 2024, p. 19). The work of Sachs and colleagues illustrates that member states' roles in the development of the toolbox are important as they are the basis for later applications.

The EU's Influence in Global Cyber Security and international law in cyberspace

The EU often emphasises its support for the international rule-based order, which it believes also applies to cyberspace (Kasper et al., 2021, p. 5). As previously established, the EU aims to address its cybersecurity issues with third states in other multilateral forums by coordinating the use of the Cyber Diplomacy Toolbox (Alatalu & Austin, 2020, p. 5).

The Cyber Diplomacy Toolbox therefore aims to foster collaboration with governmental actors and international organisations such as the OSCE, the UN and NATO (Kasper et al., 2021, p. 8), particularly regarding confidence-building measures and voluntary guidelines. The UN's voluntary norms on responsible state behaviour in cyberspace are particularly significant. Although no full consensus was reached on all the proposed norms, the EU emphasises that the preliminary results should nonetheless be respected. This commitment is pursued, for example through participation in the UN Open-Ended Working Group on cybersecurity (Attafa et Al., 2020, p. 66).

Another important cornerstone is the NATO Tallinn Manuals on international law applicable to cyber operations. These manuals stipulate that states can be held responsible for malicious cyber activities conducted against another state, particularly if they directly support, order or knowingly allow such actions to occur using their infrastructure while failing to take the necessary preventive measures to stop cyberattacks originating from their territory (Alatalu & Austin, 2020, pp. 174-175). Nevertheless, the distinction between cyberattacks and cybercrimes remains unclear, as there is oftentimes an overlap between political and economic interest of perpetrators and there is no consensus among states or in international law on which actions could prompt a response from affected states (see Poli & Sommario, pp. 526-527).

The Las Vegas Rules of responsible cyberspace behaviour assert that malicious acts should never be responded to outside of the cyber domain (Riordan, 2019, p. 27). This contrasts with the EU cyber sanctions, as set out in the toolbox, which provides for retaliatory measures against malicious cyber activities when the cyber-attack is of a similar gravity to a physical attack (Poli & Sommario, 2023, p. 530).

Nevertheless, the governance of cyberspace extends beyond responsible behaviour to encompass the technical underpinnings of the internet and ICT infrastructure. Shaun Riordan (2019) argues that the underlying infrastructures necessary for cyberspace are equally politicised as the negotiations surrounding them (p. 16). This directly links to preventive measures within the Cyber Diplomacy Toolbox, as the EU has the potential to export its standards abroad, either through capacity-building and awareness-raising to prevent conflict with third countries or by promoting best practices to avoid major cyber incidents across interconnected global networks.

Capacity-building and strategic dialogue with partners are key to this. The EU's 2015 Council conclusions on cyber diplomacy call for a '*coherent international cyberspace policy that promotes EU political, economic, and strategic interests'* (Latici, 2020, p. 8). The EU maintains ten Strategic Partnerships (Latici, 2020, p. 8) reflecting how EU member states shape the cyber toolbox through Europeanisation by promoting a vision of a law-guided, values-based cyberspace that extends beyond EU borders.

The EU and NATO in cyber diplomacy

Darius Štitilis, Paulius Pakutinskas and Inga Malinauskaite (2016) show that EU and NATO's roles in cybersecurity are seen differently in member states' strategies. Belgium, the Czech Republic, Estonia, Hungary, the Netherlands and Spain explicitly mention NATO in their 2010-15 cybersecurity strategies (Štitilis et al., 2016 p. 1160). While the EU focused on increasing standards and combating cybercrime (Štitilis et al., p. 1154), NATO focused on state-centred malicious cyber activities and standard-setting for its own organisation (Štitilis et al., pp. 1156-1157). This means that the EU and NATO generally complement each other's efforts in cybersecurity, particularly since the EU's privacy- and human rights-based approach provides a solid foundation. This should result in member states seeking different things from

NATO and the EU as well as different degrees of NATO involvement in cyber diplomacy matters, especially information sharing.

The Issues of attribution

According to the Tallinn Manuals, state responsibility can be evoked for cyberattacks that can be attributed to them or their proxies (Alatalu & Austin, 2020, p. 175). Siim Alatalu and Greg Austin (2020, p. 171) argue that the issue of attribution is affected by two new trends, namely the '*public attribution of globally spreading malware to particular states and the emergence of international coalitions of liberal democracies from around the world voicing the same political message*' (Alatalu & Austin, 2020, p. 171). This is both a curse and a blessing for proponents of a common EU attribution mechanism, as on one side, this gives leverage to the EU to pursue further cooperation in this regard, while on the other hand, when common attribution does not occur, individual member states might seek for coalition partners outside of the EU.

However, common attribution remains one of the major hurdles to successfully applying the Cyber Diplomacy Toolbox. As previously discussed, the EU has established an effective sanctions regime, but this mechanism can only be employed if member states agree on a common attribution of a cyberattack, providing a basis for retaliatory measures and sanctions that are justified under international law (Moret et Al., 2017, p. 4) (Ivan, 2019, p. 3). Nevertheless, the EU continues to assert that *'notifying a state that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself'* (Council, 2023(2), p. 8).

In its *'European Parliament resolution of 13 June 2018 on cyber defence (2018/2004(INI))'*, the European Parliament portrays attribution as a technical capacity issue that can be resolved through increased investment in ENISA and member states capacities, improved information sharing with NATO, and coordination with the private sector and academia to reliably attribute cyberattacks (see European Parliament, 2018). However, it avoids the main issue of political will entirely. According to Sara Poli and Emanuele Sommario (2023, p. 527), *'technical attribution is a precondition for legal attribution to an individual state organ, but it is not sufficient in itself to legally ascribe the conduct to a given state'*.

The EU seeks to detach the issue of attribution from the application of sanctions; an attack does not need to be politically attributed to a state warrant a response from the EU (Poli & Sommario, 2023, pp. 524-525). Nevertheless, the EU, can independently attribute attacks to certain individuals based on technical attribution. Attributing an attack to a specific country and thus invoking state responsibility remains the privilege of member states (Poli & Sommario, 2023, p. 528). Therefore, it can be problematic that EU member states rely on US and UK intelligence information to attribute cyberattacks. The EU could potentially fill this gap by creating an attribution mechanism whereby the EU attributes cyberattacks instead of member states (Poli & Sommario, 2023, p. 533).

The reasons why member states are hesitant to agree on the attribution of cyberattacks are varied. Firstly, they often consider it to be detrimental to their broader policy goals (see Moret et al., 2017, p. 4). Economic interests can also play an important role that prevents member states from making use of the toolbox (see Moret et al., 2017, p. 4).

Furthermore, member states may be reluctant to share sensitive information, particularly when it originates from intelligence agencies. Mutual distrust between member states persists (Moret et al., 2017, p. 3). This is worsened by the fact that not all member states possess the same level of cyber capabilities, such as expertise in digital forensics, which are necessary for credible attribution (Ivan, 2019, p. 6). Nevertheless, most states should be able to reliably attribute malicious cyber activities to certain persistent threat actors whose 'signature' is already known by using the capabilities of the private sector and the open-source intelligence community (Ivan, 2019, p. 6).

Cyberattacks affect member states in different ways, leading to varied perceptions of the severity of each incident. Digitalisation plays a different role in each member state's economy, and economic or other national security priorities may prevail over a joint EU response to cyberattacks (Ivan, 2019, p. 7). Therefore, it is conceivable that national interests and corresponding policy responses may differ based on the perception of a cyberattack. Ivan (2019) found that Italy is the most cautious of the major member states when it comes to attribution, while the Netherlands, Denmark and formerly the UK are the most active in attributing attacks and pushing for ambitious EU policy in this domain (pp. 5-7).

To address attribution-related challenges, the Cyber Diplomacy Toolbox includes actions that do not necessarily require attribution (Kasper et al., 2021, p. 8). Nevertheless, member states retain their sovereign right to make attributions individually (Kasper et al., 2021, p. 8). The issue of collective EU attribution is emblematic of the problems in the CFSP, as it requires consensus in the Council, which is often difficult to achieve, even though the High Representative for CFSP can issue unilateral statements condemning cyberattacks. In this regard, Ivan (2019, p. 9) concludes that the biggest remaining hurdle for the sanctions provided in the toolbox is the need to foster a common European culture of attribution.

The issue of attribution reveals several Europeanisation dynamics at play. Some actors seek to Europeanise the attribution process to make the Cyber Diplomacy Toolbox more effective. When this does not happen, they may choose to pursue attribution independently or in coalition with external partners, including non-EU states such as the UK (see Ivan 2019 pp. 5-6).

This issue also illustrates that member states remain the key actors within the CFSP. They can pursue national approaches and block collective EU actions if they deem them to be detrimental to their foreign policy or economic interests, or if they anticipate negative consequences, such as retaliation from the attributed state (see Moret et al., 2017, p. 4) This also demonstrates the complicated process of uploading, showing how member states attempt to generalize their own attribution of a cyberattack to the EU to create a stronger, more unified response. However, not all member states view the threat in the same way. Some may consider the response to be too strong or risky and may not support it.

Can effective cyber deterrence exist without hard power?

Cyber deterrence is repeatedly evoked by the EU in the documents of the Cyber Diplomacy Toolbox, to ensure safety by fear of retaliation (see for example Council, 2019(2), p. 8 or Council, 2017(1), p. 4). The EU is an entity of international law that can act independently of its constituent states (Poli & Sommario, 2023, p. 524). Regarding the global distribution of power in cybersecurity, Agnes Kasper, Anna Molnár and Anna-Maria Osula conclude that, unlike major cyber powers, the EU lacks hard cyber capabilities, calling into question the possibility of credible cyber deterrence being exercised by the EU (Kasper et al., 2021, p. 5). Similarly, Riordan (2019, pp. 30-31) underscores the importance of tangible retaliatory actions for effective cyber deterrence. However, the EU must instead rely on its norm-shaping role and

persuasive abilities, which are significantly bolstered by its economic might (Kasper et al., 2021, p. 5). However, the EU itself seeks to contrast this opinion, stating that the consequences outlined in the Cyber Diplomacy Toolbox, which operate outside of the cyber domain, serve as an effective real-world deterrent through the use of diplomatic and political means, as well as economic sanctions (Kasper et al., 2021, p. 8).

The literature is split on whether the toolbox can effectively deter cyberattacks. Sachs et al. (2024, p. 22) find that the toolbox itself is insufficient for effective retaliatory deterrence. Poli and Sommario (2023, p. 524) argue that the measures in the toolbox do not have a 'punitive purpose' as this can only be achieved through Member state cybercrime legislation, however the measures in the toolbox could potentially prevent future attacks.

3. Theoretical Framework

The work is based on the Europeanisation of foreign policy theory, as set out by Reuben Wong and Christopher Hill (2011) and Ben Tonra (2015), classical Europeanisation theories as exemplified by Liesbet Hooghe and Gary Marks (2019), Andrew Moravcsik (1998), and Ernst Haas further developed by Ben Rosamond (2005) to formulate logics behind the axes observed.

According to Wong and Hill (2011, p. 13) and Tonra (2015, p. 188), Europeanisation in CFSP does not necessarily entail convergence towards a unified European foreign policy, but rather some form of adaptation to Europe. According to Wong and Hill (cited by Tonra, 2015, p. 190), several factors lead to Europeanisation: *'institutions and treaties, socialisation, leadership, external federators, the politics of scale, legitimisation of global roles, and geo-cultural identity'* (Tonra, 2015, p. 190), as well as opposing factors such as *'ideological hostility, domestic politics, international forces, and special relationships'*. The previously mentioned patterns of argumentation are positioned below the level of the axes we observe, as part of the formulation of the national interest that underpins our axes of observation in this thesis.

However, the study of Europeanisation raises some issues. It is difficult to discern whether what we are seeing is Europeanisation and its effects or the consequence of another *'-isation'* (see Wong & Hill, 2011, pp. 11-12) (see Tonra, 2015, p. 192). It is also difficult to discern the causal relationship between Europeanisation and national policy change because they mutually

influence each other and are sometimes considered to follow a circular model (Wong and Hill, 2011, pp. 11-13). As Wong and Hill state, *'One study which claims that a Member State's foreign policy has been Europeanized is challenged by another which claims the reverse'* (Wong and Hill, 2011, p. 12). This is a complex issue and, as the downloading of positions is not examined, everything may falsely be interpreted as cases of up- or cross-loading. My rationale is that even if a position that from the EU level is included in a statement, the formulation of preferences therein still aligns with the individual priorities of the member states. For this reason, where member state preferences come from will not be investigated, even if they were firstly downloaded from the EU level, in this understanding this does not affect the self-contained processes of uploading and cross-loading.

In the following sections, the conflict between autonomy and Europeanisation in CFSP will first be explained, the three selected classical Europeanisation theories and their relationship to this conflict are discussed and finally the concepts of cross-loading and uploading are introduced.

Europeanisation-Autonomy

As part of 'high politics', foreign policy is the domain of member state competency. Member states do not take orders from Brussels (Wong and Hill, 2011, p. 210), and they even profit from the high degree of manoeuvrability and little legislation in foreign policy. Instead, Wong and Hill argue that any Europeanisation of the CFSP must occur through the alignment of values, identities, and procedures (Wong and Hill, 2011, p. 210), primarily among national elites (Wong and Hill, 2011, p. 17). However, the increasing entanglement of member state and EU goals in CFSP makes collective action necessary (Wong & Hill, 2011, p. 214), as well as more EU-level responsibilities.

Some member states may believe that the EU should present a united front (Wong & Hill, 2011, p. 216) to assert itself, whereas autonomy-oriented member states may wish to maintain their independence and avoid strictly adhering to the EU's policies (see Wong & Hill, 2011, p. 216). Therefore, they may wish to preserve the current status quo, which allows them to deviate from the EU's position when it is deemed to be detrimental to their domestic interests.

Wong and Hill provide us with a few criteria that determine the degree to which a state's foreign policy is Europeanised (see Wong and Hill, 2011, p. 211). A state trying to retain national

primacy may deviate from common EU values and positions in multilateral fora and bilateral negotiations when these are detrimental to the national interest, rather than pursuing its national foreign policy through collective EU action. In contrast, a state with a Europeanised foreign policy may be seen to take common EU standpoints in its own foreign policy, even in bilateral meetings with third countries or in other multilateral forums. Being part of the EU may form part of its diplomatic posture, leading it to pursue its own foreign policy through collective EU action (see Wong & Hill, 2011, p. 211). It is important to note that these criteria, adapted from Wong and Hill, are used to measure the Europeanisation of member states' domestic foreign policies, i.e. downloading rather than uploading or cross-loading and must be adapted to better fit the case of the toolbox. Therefore, based on Wong and Hill's work, Europeanisation is defined more broadly, focusing on support for common European action and potential transfer of powers, and autonomy as opposition to common action and support for the retention of member state sovereignty and powers.

Classical Europeanisation Theories

In *Grand Theories of European Integration in the Twenty-First Century*, Hooghe and Marks (2019) note from the outset that these three theories, neofunctionalism, intergovernmentalism, and postfunctionalism, are not necessarily mutually exclusive. Due to their adaptability, they are difficult to disprove entirely (see p. 1113). The challenge lies in determining which theory best explains the observed phenomena.

Postfunctionalism

Postfunctionalism introduces the concept of identity into the realm of European integration (Hooghe & Marks, 2019, pp. 1116, 1122), which may result in economic irrationality, where nationalism takes precedence over economic interests (Hooghe & Marks, 2019, p. 1124). Postfunctionalism recognises that issues can be politicised at various levels, including the intergovernmental and EU levels, as well as the realm of mass politics, where issues can escape elite negotiations and become the subject of political debate by civil actors and the media (Hooghe & Marks, 2019, p. 1117). EU member state governments are aware that there are multiple arenas beneath the governmental level (Hooghe & Marks, 2019, p. 1119), meaning that nationalist sentiment could be leveraged to validate opposition to further integration efforts (see Hooghe & Marks, 2019, p. 1128). In cases such as the negotiations on the toolbox, where

nationalism and international governance clash (Hooghe & Marks, 2019, p. 1124), post-functionalism also accounts for disintegration (Hooghe & Marks, 2019, p. 1117).

Regarding the Cyber Diplomacy Toolbox, postfunctionalism could offer valuable insights into the reasoning behind the nationalisation process behind the 'autonomy' code, in a scenario where nationalist forces within the member states‘ sphere advocate for the maintenance of member state primacy in CFSP matters, and consequently, the measures outlined in the toolbox, particularly the critical issue of attribution.

In contrast, postfunctionalism can also explain that if negotiations concerning the Cyber Diplomacy toolbox have not yet become a component of the domain of mass politics, it can be deduced that the economic interests of the elites persist as the predominant driving forces. This is because the identity and sovereignty narrative has not yet been initiated, and so Europeanisation can progress unhindered.

Intergovernmentalism

According to intergovernmentalism, the member states are central actors within international politics (Hooghe & Marks, 2019, p. 1120), seeking economic gain through intergovernmental bargaining (Moravcsik, 1998, pp. 6-7). Moravcsik (1998 p. 4) separates the driving factors of intergovernmentalism into three steps: *'economic interest, relative power and credible commitments'.* Hooghe and Marks reformulate this into three steps: *'the domestic formation of national preferences; intergovernmental bargaining; and the creation of European institutions to secure agreements'* (Hooghe & Marks, 2019, p. 1116).

The curtailment of the geopolitical power of European states plays only a marginal role in intergovernmentalism (see Moravcsik, 1998, p. 4). Rather, economic interests supersede this, and only where economic interests are weak can other interests prevail (Moravcsik, 1998, p. 7). For the Cyber Diplomacy Toolbox, this could be a useful lens through which to interpret the process of Europeanisation, given that the fear of economic damage caused by cyberattacks incentivises cooperation. According to intergovernmentalism, states are unlikely to relinquish their sovereignty without receiving some form of economic benefit in return (Moravcsik, 1998, p. 3).

A core tenet of intergovernmentalism is that power among states is determined by 'asymmetrical interdependence' (Moravcsik, 1998, p. 7). This may result in 'lowest common denominator' politics (Hooghe & Marks, 2019, p. 1116), whereby, according to Moravcsik

(1998, p. 3), states with a lot to gain (in our case, those with highly vulnerable economies to cyberattacks) should be the strongest proponents of passing a common policy. In contrast, states with only marginally affected economies can use their veto rights to set the pace (see Moravcsik, 1998, p. 3).

According to Moravcsik, the creation of further EU-level competencies in intergovernmentalism is intended to ensure compliance among the member states (Moravcsik, 1998, p. 9). In the CFSP, however, member states may be incentivised to deviate from these competencies as they fear few tangible consequences (see Hooghe & Marks, 2019, pp. 1121-1122). The economic nature of integration in intergovernmentalism makes disintegration unlikely (Hooghe & Marks, 2019, p. 1124), even when national sentiment is strong (Hooghe & Marks, 2019, p. 1115), due to economic interdependence acting as a mediating factor (Hooghe & Marks, 2019, p. 1124). Intergovernmentalism explains high-level negotiations between national leaders as driving further integration, with the leaders themselves arguing based on domestic preference.

In this scenario, the value of intergovernmentalism is explicitly given in my research question: by focusing on the member states and their preferences, intergovernmentalism becomes an important lens through which to view the issue. States at higher risk from cyberattacks by third states may pursue a Europeanised policy emphasising cooperation and joint action, as well as greater EU-level powers, to help mitigate the economic risk they cannot reasonably defend against alone. States with relatively little risk from cyberattacks by third states may be wary of retaliatory responses, such as sanctions on their economies from affected countries. They would therefore prefer to retain member state primacy and act on a case-by-case basis according to their perceived national interest.

Neofunctionalism

Neofunctionalism and liberal intergovernmentalism share some core similarities (Rosamond, 2005, p. 243) such as the fact that domestic interest remains the key driver of integration (Schmitter 2006, p. 259). Neofunctionalism is based on the idea that Europeanisation is driven by interdependence and shifting loyalties (see Rosamond, 2005, p. 246), as opposed to security imperatives (see Rosamond, 2005, p. 240). Neofunctionalism forms part of pluralist political science, actors of civil society are perceived to help create state preferences or may choose to pursue their goals by bypassing states and engaging directly at the European level (Rosamond,

2005, p. 241). However, in the CFSP, this possibility is relatively limited. Conversely, pluralist societies may be more inclined to integrate with the European level to best serve their organised interests (Rosamond, 2005, p. 241).

Actors and governments have limited understanding of the consequences of the actions they pursue at EU-level (Schmitter, 2006, p. 259) as well as a limited time-horizon to make decisions (Hooghe & Marks, 2019, p. 1115), which may affect their preference formulation. Neofunctionalism is a useful theory for explaining why supranationalisation progresses during crises (see Hooghe & Marks, 2019, p. 1120), when the effective provision of common goods or outcomes is threatened (see Rosamond, 2005, p. 249) (see Schmitter 2006, p. 259). In this scenario, member states would need to collaborate to provide the public good of cybersecurity, and they might decide to delegate the management of this public good to the EU's supranational authority as an expression of regional integration. According to neofunctionalism, this process occurs due to increased interdependence, which is partially caused by further economic relationships that reinforce supranationalisation (Hooghe & Marks, 2019, p. 1114). This interdependence is also due to dependence on expertise and implementation derived from the supranational authority (Hooghe & Marks, 2019, p. 1114). This is relevant for the example of the Cyber Diplomacy Toolbox where expert knowledge is especially important.

Rosamond (2005, p. 251) frequently underlines the adaptability of neofunctionalism and the overall work of Haas. In response to intergovernmentalist criticism in the 1960s, Haas emphasised the significance of 'exogenous stimuli' (Rosamond, 2005, p. 248) for effective integration. These stimuli encompass societal, external and ideational preconditions of integration (Rosamond, 2005, p. 249), underscoring the importance of external factors in facilitating integration processes. It is therefore conceivable that the absence of these stimuli as preconditions for successful Europeanisation, would result in the retention of autonomy and national sovereignty.

Spillovers

Rosamond (2005, p. 244) defines spillovers as the shift in expectations towards further EU integration. This occurs when actors recognise newly created supranational centres of authority as providers of results that align with their preferences, leading to harmonisation. I interpret spillovers as the necessity for further supranational integration and cooperation, arising from functional pressure exerted by policy areas where integration has already advanced

(Rosamond, 2005, p. 244; Hooghe & Marks, 2019, pp. 1114-1115). I understand this as a self-reinforcing domino-effect whereby the effective implementation of Policy A necessitates further integration in the form of Policy B.

The significant steps taken in recent years in EU-level cybersecurity management, such as the NIS directives may make it sensible to strive for further EU-level competencies regarding the development of the CFSP. Spillovers can also be 'cultivated' (Rosamond, 2005, p. 245), whereby institutions pursue further integration independently. The presumed particularity of the CFSP is that, unlike in other areas, the Commission cannot promote supranationalisation as effectively through its own agenda (see Hooghe and Marks, 2019, p. 1125); the member states play the leading role in the CFSP. Spillover is also possible, particularly when it is cultivated by Council presidencies or the EEAS (see Stephenson, 2010, p. 1043). Poli & Sommario (2023, pp. 532-533) describe that the EU has asserted its authority in the field of cybersecurity by basing its argument for new rules and harmonisation between member states on the increased interconnectedness of markets and security. I argue that from a neofunctionalist perspective, this would be a typical example of a spillover effect described.

According to neofunctionalism, crises may temporarily halt further integration, but the overall direction towards more supranationalisation prevails (Hooghe & Marks, 2019, p. 1115; see also Schmitter, 2006, pp. 257-258). However, crises, as manifestations of external stimuli, do not necessarily hinder further integration. Sometimes, external crises and the ensuing pressure to act can empower integrationist forces (Rosamond, 2005, pp. 248-249; see also Hooghe and Marks, 2019, p. 1121). Path dependence can help to explain why the costs of regression may still be higher than those of continuing integration (see Hooghe and Marks, 2019, p. 1121). Neofunctionalists might argue that effective supranationalisation can occur in response to external pressures or through spillover effects resulting from prior European integration. According to the logic of path dependence, an effective common attribution scheme becomes useful due to the pressure towards an effective cyber diplomacy regime necessary for the toolbox itself to work. From a neofunctionalist perspective, we should therefore expect to see a trend towards further Europeanisation relating to the Cyber Diplomacy Toolbox due to path dependence and spillovers.

Ramifications for the Cyber Diplomacy Toolbox Development

This section illustrates what member states' behaviour can be expected by the selected classical Europeanisation theories. As Hooghe and Marks (2019, p. 1113) say, theories are adaptable and hard to disprove, so arguments can be made for every category.

Table 1: Potential expectations

Theory	Autonomy	Europeanisation
Postfunctionalism	MS argue based on a nationalist sovereignty discourse / refer to political will expressed by nationalist forces domestically to oppose common action.	The issues of the Cyber Diplomacy Toolbox have not yet escaped from the 'elite-arena' and remain a technocratic issue where economic/elite interest prevails.
Intergovernmentalism	MS are unwilling to harm their (economic) relationship with 3rd states through collective sanctioning that does not align with their self-interest.	MS economies are threatened by cyberattacks and MS hope to protect them by deterring attacks through collective action.
Neofunctionalism	In the absence of exogenous stimuli, social preconditions, or cultivation of spillover Europeanisation does not progress, and MS choose to retain their autonomy.	MS elites have shifted their loyalties towards the EU and pursue common action and even supranationalisation for economic reasons, as well as due to external pressures, as they do not expect MS governments alone to provide satisfactory results. Previous integration in fields such as Defence, Common Market and Cybersecurity create spillover pressure towards harmonisation for policies to be effective.

Uploading and Cross-loading

Europeanisation can be presented as either the dependent or the independent variable (Tonra, 2015, p. 188), and it can be regarded as either a theory or a process to be studied. In my case,

I regard Europeanisation as a theoretical lens through which to understand the behaviour of member states in CFSP, as exemplified by the development of the Cyber Diplomacy Toolbox.

The processes that make up Europeanisation are commonly seen as uploading, cross-loading and downloading. Wong and Hill (2011, p. 4) define uploading as bottom-up Europeanisation, downloading as top-down Europeanisation, and cross-loading as a bidirectional process (Wong & Hill 2011, p. 4) among member states with the goal of influencing other member states to ultimately change common policy (see Aggestam & Bicchi. 2019, p. 519).

For the purposes of this work, I will not examine downloading in detail, as I consider this process to be more relevant to the analysis of the toolbox's application than its development. My research question explicitly targets the influence that the member states have exerted on the toolbox. However, it does not consider the impact of the toolbox on national member state policy. The Europeanisation of member states national foreign policies often involves adapting domestic foreign policy according to the common European standpoint (Tonra, 2015, pp. 190-191). This is what is considered downloading. I will focus only on uploading and cross-loading, as these ultimately deal with influencing EU-level policy, whereas downloading deals with member state-level policy change.

Uploading

The guiding question for uploading is '*Which positions might the EU not have developed without impetus from one or more particular states?*' (Wong & Hill, 2011, p. 214).

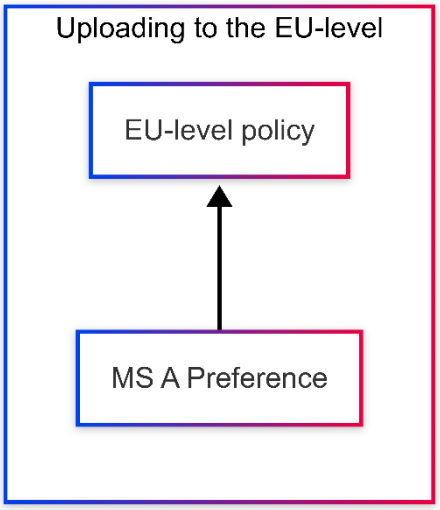
In foreign policy, EU institutions only have limited influence at the EU level (Tonra, 2015, p. 185) (Wong & Hill, 2011, p. 17) as there is little EU-level legislation binding the member states (Tonra, 2015, p. 185) (Wong & Hill, 2011, p. 17). In relation to the CFSP, Tonra defines uploading as *'when and to what end national foreign-policy preferences are brought to the European table and pursued using the EU as a means of amplifying national foreign policy'* (Tonra, 2015, p. 184). It is generally accepted that member states seek to upload their domestic policies to the EU level (Tonra, p. 185) (Wong & Hill, 2011, p. 1), in a process described as *'the European rescue of national foreign policy'* (Allen, 1996; Milward, 1992, cited by Tonra, 2015, p. 185), or as *'efforts to increase the state's global profile, influence EU partners' foreign policy, and use the EU as a shield/umbrella for national policy and an influence multiplier'* (Wong & Hill, 2011, cited by Tonra, 2015, p. 186). According to this understanding, EU foreign policy is the dependent variable constituted by the combined interests of the member

states' national preferences. Europeanisation progresses through the perceived need to fulfil the rational self-interest of the state via the megaphone of the EU. Member states retain a distinctive self-interest, amplified through uploading.

A second interpretation of uploading suggests that self-interest is influenced directly from the top down by the European level and vice versa (see Tonra, 2015, p. 186) (see Wong and Hill, 2011, pp. 1-2). According to Tonra (2015, p. 186), European and national policies are in a reciprocal relationship with each other and mutually influence each other (Wong & Hill, 2011, p. 10). Tonra (2015, p. 186) describes how, from this perspective, creating a common European standpoint becomes a national policy preference of member states rendered necessary by the assumption that achieving the national policy goal requires common action due to spillovers from other fields. In this case, the advantage of collaborating with EU partners or granting additional EU-level competencies serves the national interest, while retaining veto rights in CFSP (Tonra, 2015, p. 187). Wong and Hill conclude that foreign policy, even if part of member state competencies, is not immune to the process of Europeanisation (2011, p. 10).

The definition of uploading that will be used is like that used by Tonra (2015, p. 184). It is broader in that it considers policy preferences rather than focusing solely on the uploading of specific policy examples from national levels. In its simplest form, uploading occurs when a single member state seeks to pass EU-level policy based on its preferences, which can then become binding for all other member states. A fundamental issue when it comes to identifying uploads is that it is not always known which proposals stem from national priorities and whether the intention is to influence EU-level decisions. Therefore, for the sake of simplicity, it is assumed that member states generally act in accordance with their national preferences; otherwise, they would probably not pursue a particular policy. As an indicator of uploading, I have chosen to focus on language that clearly indicates a preference for a change at EU level. For example, member states seem to be very aware of the difference between using 'could' or 'should' in a paragraph and 'welcomes' compared to 'takes note of'. Such formulations are used as indications of policy preference formulation and uploading. In other cases, member states make statements using language that clearly indicates their priorities, such as referring to themselves in the third person, for example: 'Austria would like to reiterate that...'. However, certain cases do not constitute uploads. For example, matters that are clearly not related to a policy preference, such as grammatical changes that do not have an explicit meaning, are not included.

Figure 1: Uploading



Cross-loading

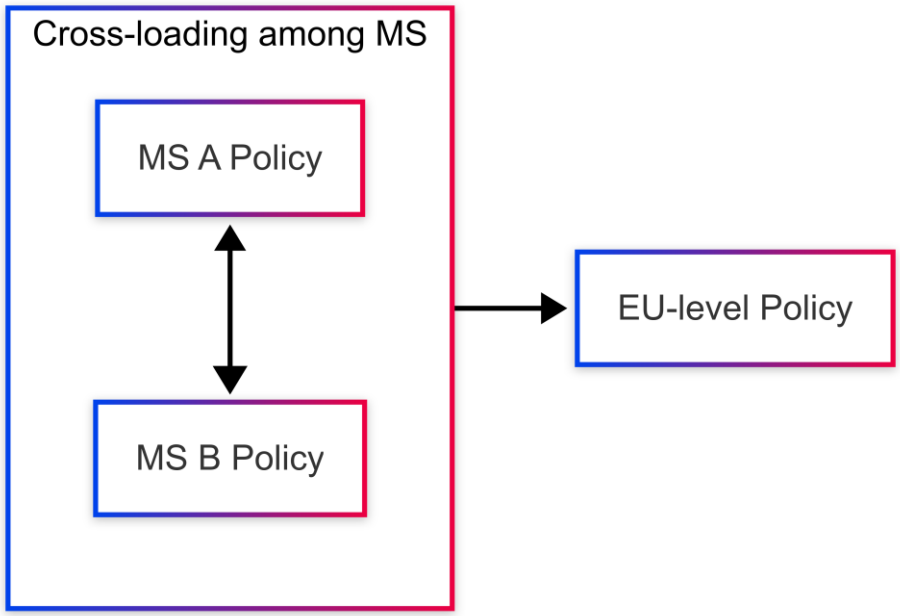
Regarding cross-loading, early theories on the development of Europeanisation in foreign policy predicted an increasing Europeanisation of member state foreign policies based on shared information and views among member states (Tonra, 2015, p. 186). According to Tonra (2015, p. 184), cross-loading in the CFSP is the process whereby member states draw on each other's examples of policymaking structures, information, and analysis to formulate their own policy preferences. Wong and Hill (2011, p. 214) define cross-loading as the transfer of ideas and procedures between member states. The difficulty lies in identifying which ideas have passed through the EU to reach the member state level and which have been transferred directly between member states bilaterally. In its simplest form, Aggestam and Bicchi, in reference to Wong and Hill (2011) and Tonra (2015), define cross-loading as '*the mutual influence among Member States, independent of mediation by EU actors'* (2019, p. 515). In the context of the Cyber Diplomacy Toolbox, the recurring theme of sharing situational awareness, policy proposals and information related to the attribution of cyberattacks can constitute cross-loading, benefiting from member states with more experience in cybersecurity and cyber diplomacy. Cross-loading contributes to the emergence of common interests (Tonra, 2015, p. 187) that may align multiple member states due to their shared informational environment.

Aggestam and Bicchi (2019, p. 519) argue that leadership can influence cross-loading. In these cases, certain actors seek to guide common activities, for example when member states make suggestions that are then adopted by others. Cross-loading involves like-minded EU states

forming groups (see Aggestam & Bicchi, 2019, p. 515). These groups collectively advocate for a certain policy and actively exchange information with each other, for example when they jointly write a whitepaper. Their national policy preferences align based on common policy preferences, following the leadership of another member state or shared information. Also, it is not necessary for member states to agree for cross-loading to happen, as a bidirectional process between two states: *'They may emulate, distance themselves from, or relaunch a practice'* (Aggestam & Bicchi, 2019, p. 519).

The definitions of cross-loading by Wong and Hill, Tonra and Aggestam, and Bicchi all focus on the informality of cross-loading. While the above definitions undoubtedly underpin cross-loading, identifying it in the coding of statements in this thesis would be difficult due to its informal nature. Ultimately, it leaves too much room for speculation and interpretation of processes. Therefore, I propose to define cross-loading as the information exchange between member states without concrete EU interference, like the definition used by Aggestam and Bicchi, but only in cases where there is clear collaboration between member states or where states explicitly refer to the positions of other member states. In the context of the Cyber Diplomacy Toolbox, cross-loading is identified by examining references made by one member state to the policy or preference of another. It is also identified by occasions where collaboration has taken place without the EU acting as an intermediary, which indicates that an information exchange has occurred. In other words, I look for occasions where member states noticeably reference the policy suggestions of other member states.

Figure 2: Cross-loading



4. Methodology

Research Design

To answer our questions about the influence of member states on the development of the Cyber Diplomacy Toolbox, I propose the following research design. I will conduct a qualitative text analysis of the corpus assembled through a keyword search of online sources. These sources include both primary EU sources and news from EU-focused media. However, they do not include statements made by EU entities on the development of the toolbox, unless they reference the role or advocacy of specific member states, nor statements made by member states outside of an EU context regarding the toolbox such as member state domestic cybersecurity strategy papers.

I follow Udo Kuckartz's (2014, p. 63) approach of deductive category construction, meaning that the codes and categories are derived from the theory outlined above, rather than from the corpus itself. Although I am tempted to apply deductive-inductive category construction (see Kuckartz, 2014, p. 70), where we first approach with categories derived from theory and then saturate them with data and adjust the categories accordingly. I opt for this method as I am concerned that I would end up with too many categories o be useful, given the size of the corpus

I can work with. I am therefore arguing for a rigid measuring stick, outset from the start, instead of moving the goalposts later. Nevertheless, statements should still be grouped according to argumentation patterns. This is handled as a distinct process beyond the initial five categories.

I justify the use of this method by citing Benoit (2020, p. 476): "*Qualitative text analysis is labour-intensive, but it leverages our unique ability to understand raw textual data, providing the most valid means of generating textual data. Human judgement is the ultimate arbiter of the 'validity' of any research exercise* ". This is useful for this case, as the corpus consists of a heterogenous mix of diplomatic correspondence and news sources, which means that only with adequate rhetorical and contextual understanding can coding be done reliably and the meaning be understood.

Data Collection and Corpus

The corpus was compiled from documents on the EU Council website, and media sources mainly Agence Europe and Euractiv. Where relevant, I have also used files cited or linked in the above sources that are not available in the sources alone. For example, non-papers referenced in a Council document that are only available on a member state's Ministry of Foreign Affairs website. I have also conducted Google News searches using inputs from other news agencies on stories covered by both Euractiv and Agence Europe. These are, however, only included in the corpus in two cases: one where Euractiv collaborated with other press agencies on a story, and another is where Politico provided access to a relevant non-paper. I left other news articles aside, as they were mainly reporting on the same stories. News sources also mentioned the presidential priorities of certain member states about cyber diplomacy. Notably, there was a lengthy article on the French Council priorities. This was used as an entry point to examine all the Council presidential priorities that explicitly mention the Cyber Diplomacy Toolbox, not just the ones referenced by the news sources. This added the Danish, Belgian, Swedish and Hungarian priorities. These were also considered, despite them not being mentioned in the news sources, as they are directly relevant to the issue of the toolbox and function like statements made at Council level as they deal with promotion of the toolbox.

Keyword searches were used on these websites to identify relevant documents. Keywords include 'toolbox', 'cyber sanctions', 'cyber diplomacy', 'digital sanctions', 'digital diplomacy' ' cyber' and 'cyberdiplomacy' and truncations thereof.

Two criteria were used to define what is relevant for inclusion in the corpus: does the entire document deal with Cyber Diplomacy Toolbox, or does only a specific statement or paragraph deal with cyber diplomacy? Based on this, either multiple statements of documents that deal entirely with cyber diplomacy, even if cyber diplomacy is not explicitly named in the paragraph but it remains relevant, or just single paragraphs that explicitly deal with cyber diplomacy and toolbox actions, if the main topic is not cyber diplomacy of the entire document, were chosen.

The analysis covers the period from 2017 to 2025, which includes the official adoption and subsequent development of the toolbox. Research was conducted on the Agence Europe website using these keywords, yielding a broad set of results (over 500). Articles were then selected based on titles referencing the cyber toolbox or related aspects. A preliminary reading was performed to assess their relevance, resulting in a final set of relevant articles from Agence Europe (32 files) and Euractiv (43 files) dealing with cyber diplomacy, as well as a file from Reuters, which was done in collaboration with Agence Europe. These files were filtered again to remove duplicate news stories. For example, Euractiv published some articles multiple times, but in a brief as well as the the article. Cases where member states were not clearly identifiable were also removed, as it is imperative that member states can be identified due to the explicit focus on the role of member states in the research question.

Working with the corpus presented difficulties due to many seemingly relevant articles referencing aggregated statements on the development of the toolbox without mentioning individual member states. These files were read thoroughly to ensure that no links or references to other files, which could provide additional information concerning explicit linkages to member states, were overlooked. Ultimately, however, statements were only coded if it was possible to attribute a member state to the position or statement mentioned in the article. As the research question explicitly focuses on the preferences and behaviours of member states, statements lacking this information cannot be included.

Two of the most important documents are *8146/1/17 REV 1* and *8907/17*, which detail the amendments made by the delegations to the 2017 *Council Conclusions on a Joint Diplomatic Response to Cyber Operations (Cyber Toolbox)*. These two documents seem to offer the closest insight into the tangible preferences of member states and form a major basis for the corpus. In addition, I consulted the *Working Paper on the 2021 draft Council Conclusions on the EU's cybersecurity strategy for the digital decade*. While this document is not one of the main

documents establishing the Cyber Diplomacy Toolbox, it includes statements and changes made by member states on the paragraphs of the text relating to the toolbox and its application. This provides valuable insight into their policy preferences and behaviour on the topic.

Coding operationalisation

I divided the coding scheme into three axes: 'common response' (autonomy-Europeanisation), 'reasoning pattern' (uploading and cross-loading) and 'spillover'. Due to the heterogeneous nature of the statements, much of which use rather diplomatic language that requires context to understand, using only specific words alone as indicators proves insufficient.

Indicators of Europeanisation are expressions of support for a common European response by EU member states regarding cyber diplomacy. In the strongest cases, this can also include a specific delegation of powers to the EU or, in weaker cases, an absence of opposition to such a delegation or a call for coordination and development at EU level of the toolbox and its measures. Europeanisation can also be expressed through calls for the application of the toolbox, as this amounts to support for common EU action.

In contrast, the autonomy code includes statements that primarily base themselves on national sovereignty or established competencies to explicitly oppose the transmission of powers to the EU or the application of toolbox measures based on such a narrative.

The uploading code is guided by the question, '*Would the EU have developed this position independently without member state intervention?*' (Wong & Hill, 2011, p. 214). The strongest expressions of uploading clearly refer to a national policy or priority that they want to be integrated into EU policy. As previously said it is impossible to know exactly what the member state priorities are before their articulation, it is assumed that all cases in which member states introduce meaningful changes to EU texts are consistent with their priorities.

As cross-loading is based on the exchange of information between member states, the indicators for cross-loading are, in most cases, actions carried out together with other member states,. In other cases, cross-loading can entail explicit references to suggestions from other member states. These references do not have to be positive; the defining factor is the information exchange.

Finally, statements marked with spillover include all mentions of policy fields or policy goals that are not strictly cyber diplomacy, aiming at an expansion of the EU's competencies or linking existing policies in other policy fields with cyber diplomacy, creating the need for further action. Spillover can go both ways: sometimes, effective cyber diplomacy requires action in the form of further commitments or connections to other fields. In other cases, other fields need enhanced cyber diplomacy efforts to be able to secure themselves and meet their policy goals, thus validating the expansion of the toolbox.

Coding Process

The coding was done in Microsoft Excel for the five categories: autonomy, Europeanisation, uploading, cross-loading and spillover. Relevant contextual information about the text was provided, such as authorship, as well as my reasoning for the coding. A second round of coding was then conducted on the same statements to compare the codes and generate the final dataset. To avoid implicit bias when allocating certain member states to 'roles' in relation to the toolbox, the second round of coding was done with the authorship of the statements concealed and in a different order. The two versions were then checked for discrepancies in the codes to create the third coding table. In this version, some statements were removed that were not specific enough to the Cyber Diplomacy Toolbox.

Dealing with track changes

Some of the relevant statements I found as part of the working documents, took the form of changes introduced by a member state to a proposed text. In this case, states were asked to fill in their wording and policy preferences and cancel out what they did not agree with. Extracting meaning from such paragraphs is more interpretative than from 'direct' statements, such as those found in news articles or white papers. To help structure the process of extracting meaning from such comments and track changes, I have devised the following three-step process.

Firstly, look at comments and other information accompanying the changes, such as a foreword explaining the overarching motif between changes.

Secondly, look only at the changes made to the paragraph, what is being changed, and which narrative would this fit.

Thirdly, look at the whole paragraph, comparing the unchanged version with the changed version.

It is more important to consider the comments and changes written by the individual member states, as these are arguably closer to their preferences. It is better to avoid considering entire paragraphs where possible, as these are often co-authored by sources such as the Presidency or the EEAS rather than the member state itself. It is only through looking at the member state changes that it can be 100% assured that the authorship corresponds to the member state in question.

Defining the field of cyber diplomacy in contrast to cybersecurity and hybrid threats.

What is common in the statements is that cyber diplomacy matters are very frequently named in the same sentences as cybersecurity and hybrid threats. Most frequently, associated with documents such as the hybrid toolbox or the NIS directives and bodies created thereof, see for example:

(Germany) *"In addition, it should be discussed in how far the EEAS's Hybrid Fusion Cell can be used as focal point for voluntary information and intelligence sharing on cyber operations that require an EU diplomatic response. The Hybrid Fusion Cell may be the appropriate venue to coordinate information sharing also on cyber operations, as cyber operations are particularly useful tools in hybrid conflicts "(*Council, 2017 (3), p. 14).

Cyber diplomacy is distinct from the fields of cybersecurity and hybrid threats. It can be defined as a set of tools and communication strategies aimed at third parties to ensure cybersecurity and respond to hybrid threats. Cyber diplomacy encompasses all responses to such issues via foreign policy. This definition is especially important when considering spillover: based on the previous definition, changes argued based on issues that are very closely related, such as cybersecurity, defence and the economy, constitute spillover into the realm of cyber diplomacy.

Member states do not always clearly distinguish between the fields of cybersecurity, hybrid threats and cyber diplomacy, cross-referencing these fields in their statements, which creates ambiguity in the texts regarding what is being discussed. To distinguish between these fields and clearly delineate what is relevant to my research question concerning the Cyber Diplomacy Toolbox, only those instances are coded in which the cyber sanctions regime or the Cyber

Diplomacy Toolbox are explicitly mentioned in the context of hybrid threats or cybersecurity. Similarly, cases were included where member states use the term 'digital diplomacy' when referring to topics that would fall more within cyber diplomacy according to the definition used.

5. Comparative Patterns of Europeanisation and Autonomy

The results on Europeanisation and autonomy are varied. From the corpus, I found that Europeanisation was the defining factor in most of the statements I researched. Overall, there are 204 statements recorded in the corpus. These statements vary widely in length and in the intensity of preference they present. For this reason, I would caution against conducting a quantitative analysis of these statements beyond gaining a general overview of the corpus. Of these statements, 138 expressed support for Europeanisation and common action among EU member states, 38 expressed support for autonomy. In total, there are 105 statements coded as uploading, 41 cases of 'cross-loading', and 29 cases of 'spillover'.

The following table provides an overview of the number of 'Yes' responses for each code per state. Please note that statements shared by multiple states are counted for each member state in the table.

Table 2: Member state codes

Member State	Nationalisation	Europeanisation	Uploading	Crossloading	Spillover
Austria	0(0)	2(2)	1(1)	0(0)	0(0)
Belgium	0(0)	5(6)	4(4)	0(1)	0(0)
Bulgaria	0(0)	0(1)	0(0)	0(1)	0(0)
Czech Republic	1(1)	11(11)	9(9)	9(9)	0(0)
Denmark	0(3)	4(14)	2(2)	0(13)	0(3)
Estonia	0(3)	5(23)	1(1)	0(23)	0(12)
Finland	0(3)	3(14)	1(1)	0(14)	1(4)
France	2(2)	17(27)	16(16)	0(12)	4(13)
Germany	1(1)	9(17)	7(7)	0(10)	1(10)
Greece	0(0)	1(2)	0(0)	0(1)	1(1)
Hungary	4(4)	8(9)	9(9)	1(2)	0(0)
Italy	9(9)	2(2)	3(3)	0(0)	0(0)
Latvia	2(5)	5(15)	5(5)	0(13)	3(6)
Lithuania	0(3)	3(14)	2(2)	0(14)	0(3)

Malta	0(0)	3(3)	1(1)	0(0)	1(1)
Netherlands	8(11)	12(23)	21(21)	3(19)	1(4)
Poland	0(0)	1(11)	2(2)	0(12)	0(9)
Portugal	0(0)	5(14)	2(2)	1(12)	2(11)
Ireland	0(0)	3(3)	2(2)	0(0)	1(1)
Romania	0(3)	4(14)	0(0)	0(10)	0(3)
Slovakia	2(2)	4(6)	5(5)	0(2)	1(1)
Slovenia	0(0)	0(8)	0(0)	0(10)	0(9)
Spain	0(0)	3(4)	0(0)	0(1)	0(0)
Sweden	3(3)	7(8)	9(9)	0(1)	1(1)
UK	3(6)	1(12)	3(3)	0(15)	0(3)

Legend: Assigned codes by category and member state. Without brackets: 'Yes' values for each code where the statement is attributed to one member state only. With brackets: 'Yes' values for each code where the statement is attributed to one member state only in addition to '*Yes' values for each code where the statement is attributed to multiple member states at once.Example: there are five 'Yes' values for Estonia concerning the 'Europeanisation' code for a statement made by Estonia alone. As there are 18 additional statements made by Estonia with other member states that have this code, the numbers of 'Yes' with and without brackets are 5 (23).*

Tacit acceptance

Throughout the coding process, it was found that certain statements took a stronger stance on the issue of the Cyber Diplomacy Toolbox than others and were more relevant to it. This is because they either express strongly formulated preferences or fit very well within the coding scheme.

During the final phase of the first coding cycle, teal-blue markings were introduced to the coding scheme for 'tacit acceptance'. Tacit acceptance means that member states resubmit unaltered texts received from the EU level as part of packages of texts intended for larger documents. This means that the member state delegation has read the text and deemed it acceptable without changing it to fit their preferences. While these cases of tacit acceptance are statements in themselves, as they involve a member state agreeing to and submitting a text, they deserve to be considered separately, as there is no clear evidence of a member state making changes or additions. The primary use of teal-blue coding can be found in the comments on the Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade. Here, member states submitted the entire draft conclusions text multiple times, including the changes and comments they wanted to see implemented. However, not all member states amended the relevant parts on the Cyber Diplomacy Toolbox mentioned in the text; some simply left it

unchanged and resubmitted it. In theory, this still constitutes a statement out of which a preference can be extracted, as it is a text submitted by a member state on the topic of the toolbox and cyber diplomacy. Tacit acceptance markings set these statements apart from statements where member states expressed themselves freely. Some member states submitted slightly altered paragraphs, making changes to the grammar. These cases were also considered to be tacit acceptance if there was no discernible meaning behind the grammatical change other than correcting an error.

Application of the toolbox as an expression of Europeanisation.

Some of the statements relate not only to the development of the toolbox, but also to its application. As this is not an in-depth analysis of the toolbox application, it was considered whether these instances should be included. Nevertheless, these cases are important sources of statements and instances where the development of the toolbox is pursued and where member states consciously express Europeanisation and the uploading of national preferences.

The cyber sanctions regime was implemented following the WannaCry and Cloud Hopper attacks, targeting the Russian GRU and entities in China and North Korea (Gessant, 2020, p. 1). Following the attack against the Organisation for the Prohibition of Chemical Weapons, member states called for its implementation (Gessant, 2018, p. 1), prompting further development of the EU's sanctions regime. However, European leaders refrained from attributing the attack to Moscow, instead singling out the GRU for sanctions. In response to the 2020 cyberattack, Germany issued arrest warrants in 2021 and used the regime to sanction perpetrators. In the wake of the 2021 attacks on Poland and Ireland (Gessant, 2021, p. 1), calls for the toolbox's application grew. Poland attributed the attacks to Russian persistent threat actors, while Ireland was hesitant to support the tool. Poland emphasised the attack's EU-wide implications, while Ireland refrained from direct advocacy for its use.

Calls for the application of the toolbox that can be attributed to a member state were coded. Europeanisation is not merely about the creation of instruments, but also about utilisation and acceptance of the mechanism, which can then lead to further development of the toolbox. In these instances, a member state is pursuing a shared response at the EU-level and searching for EU-coordination in line with its national preference.

On the 2018 and 2020 non-papers

The non-papers were treated separately from the other statements because it is possible to attribute contributions to several member states, which warrants their inclusion in the corpus. However, it is not possible to clearly attribute specific positions to individual states. The statements from the non-papers are best served in a designated section in the text, and not as part of individual state sub-chapters to avoid unnecessary repetition for each member state. As the non-papers are addressed in their respective sub-section, the number of statements in Table 2 differs from the number in the individual country sections. Statements from the non-papers are not addressed in the individual country sub-sections unless there is an argument to be made concerning the individual state, as in the case of Estonia.

The non-papers provide valuable insight into the shaping of the toolbox. Most member states that contributed to the non-papers also made direct statements about the toolbox in other documents. This leads me to believe that these states are the primary proponents of the Cyber Diplomacy Toolbox.

The 2020 non-paper contains ten statements, which are rather long, but they are coded as one statement each as they develop one coherent idea. The statements were coded as follows: eight times with Europeanisation and support for a common response, ten times with cross-loading, and ten times with spillover from other policy fields. The 2018 non-paper consists of 11 statements, with three mentions of autonomy, seven mentions of support for Europeanisation, no mentions of uploading, and 11 cases of cross-loading and nine cases of spillover.

Some of the most important instances of spillover are found in the non-papers because, due to their nature, these documents systematically seek to base their arguments on other policy fields and previous agreements to support common action. The 2018 joint non-paper, written by Denmark, Estonia, Finland, Lithuania, Latvia, the Netherlands, Romania and the UK, contains some of the most significant references to spillover and path dependency. Notably, the paper devotes an entire page to justifying the importance of a cyber sanctions regime, citing security, international law, European law, human rights and economic reasons (see DK/EE/FI/LT/LV/NL/RO/UK non-paper, 2025, pp. 1-2). Legitimation and spillover from other policy areas is a recurring theme in non-papers, as reiterated in the 2020 non-paper on cyber diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia. This paper

provides further justification for the EU to increase its engagement in cyber diplomacy, building on the reasons given in the 2018 non-paper to support the proposal for a common EU cyber policy (see Auswärtiges Amt, 2020, pp. 1-5). The 2020 non-paper devotes a designated section to the toolbox, but much of what is discussed, such as EU coordination regarding their stance in multilateral forums, EU coordination in matters of capacity building in non-EU states, and information sharing, deals with matters directly related to the toolbox and seeks to build upon it (see Auswärtiges Amt, 2020).

Interestingly, despite the general purpose of the non-papers in the case of the Cyber Diplomacy Toolbox being to support common EU action, the 2018 non-paper includes references to autonomy. These mainly refer to extracts conveying the idea that member state action should be seen as complementary to a European response and as a way of alleviating member states' fears of losing power or sovereignty: *"Cyber restrictive measure would be no different to any other type of regime; they do not stop us from utilising other response tools and they do not stop us from individually calling out those we think are responsible as we seek to change behaviour. It is necessary to include the guarantees that already exists in EU legislation, the Charter of Fundamental Rights and the case law of the Court of Justice in the cyber sanctions regime"* (DK/EE/FI/LT/LV/NL/RO/UK non-paper, 2018, p. 2).

Another notable feature of the non-papers is that they appear to have been written entirely by cross-loading coalitions, which explains why all statements were marked as cross-loading. For example, the 2018 non-paper references a Danish company (see DK/EE/FI/LT/LV/NL/RO/UK non-paper, 2018, p. 1). This suggests that there were instances of policy and information sharing among the member states involved in drafting the paper. In other words, cross-loading occurred among them without EU arbitration. According to Aggestam and Bicchi (2019, p. 515), exchanging policy points without formal EU coordination is a key component of cross-loading. On the other hand, the purpose of the non-paper is also inherently to influence those member states not involved in drafting it, which also indicates cross-loading.

Both non-papers also illustrate path dependence in neofunctionalist theory. The 2018 non-paper advocates strengthening the EU's capacity to respond to hybrid threats by building on previous developments and commitments outlined in documents such as the 2015 Council Conclusions on Cyber Diplomacy see DK/EE/FI/LT/LV/NL/RO/UK non-paper, 2018, p. 4). The 2020 non-paper bases its assertion that the EU should adopt a more unified and assertive

stance in multilateral affairs on the EU's pioneering approach in areas such as the passing of the GDPR (see Auswärtiges Amt, 2020, pp. 4-6).

Finally, the 2018 document contains an interesting example of potential spillover cultivated by the EU. The authors state that their non-paper should be considered alongside one written by the EEAS around the same time. I did not have access to the EEAS non-paper, but judging by the reference to it in the member state non-paper, it also attempted to advance the cyber sanctions regime (see DK/EE/FI/LT/LV/NL/RO/UK non-paper, p. 1).

By Country

Austria

There is relatively little content on Austria. This is limited to three statements from the Draft Council conclusions on the EU's cybersecurity strategy for the digital decade. Two of these statements were coded as tacit acceptance. Overall, it can be said that Austria did not oppose Europeanisation; none of the three statements express autonomy, but they also did not express strong support for a common EU response. Rather, based on the corpus and its composition, it can be assumed that the toolbox was considered a less significant and politicised issue and therefore not a priority for Austria. Similarly, there are no news articles that explicitly mention Austria in relation to the toolbox. Unlike Sweden (see Council (3), 2017, p. 27) at the time and Ireland (see Council, 2021, p. 74), Austria as a neutral state has not addressed the inclusion of NATO in the toolbox.

For Austria, there is one code of potential uploading, that being Austria calling for more committing language on international law in a joint EU document (Council, 2021, p. 4). This is an interesting grey-zone, concerning uploading. Although international law is not Austrian domestic policy and cannot be considered as such, the desire to adhere to international law can be considered a national priority in and of itself, as we will see with Germany and the Netherlands, constituting uploading in this case. Additionally, given Austria's hosting of multiple international organisations, the promotion of these institutions and their legal regimes could be considered part of Austria's domestic understanding of its role in the EU, Austria explicitly builds on the work of the OSCE in this area, a point that Hungary (see Council (3), 2017, p. 17) and Sweden (see Council (3), 2017, p. 27) will reiterate later. There have been no cases of spillover from Austria.

Belgium

There are six statements from Belgium, all of which express support for Europeanisation. As the holder of the EU Council presidency in the first half of 2024, Belgium was in a strong position to promote Europeanisation regarding the Cyber Diplomacy Toolbox. All the statements concerning Belgium emphasise the importance of a streamlined approach to cyber diplomacy and clearly support Europeanisation. For example, the presidency attempted to streamline the working parties dealing with cyber diplomacy issues (Bertuzzi, 2024, p. 5). Belgium was a strong advocate for the further inclusion of cyber diplomacy topics in EU foreign policy, pursuing the goal of a common EU standpoint in multilateral fora and ensuring common cyber defence and response mechanisms.

We have four instances of uploading for Belgium, mainly relating to its presidency priorities, the other two statements were not coded as uploading, as they mainly touched upon housekeeping matters in the council, which on one hand did express support for a common response in cyber diplomacy, but did not constitute uploading of a preference. The instances that were coded as uploading concern themselves with the proposed inclusion of NATO cooperation and capacity building in Africa which the presidency put ahead as priorities (see Belgian Council Presidency, 2024, p. 37).

Regarding cross-loading, we have one instance from Belgium, that being when it called for "*a "gradual response" to future attacks that could include a number of measures before sanctions*" (Guarisco, 2018, p. 2) together with other member states. The article indicates that Belgium has acted together with Sweden and Finland to suggest that sanctions should not be the first measure taken by the EU as part of the toolbox, presumably so that less escalatory measures are taken before sanctions are used as a last resort. Overall, this is consistent with other statements from Belgium, which has mainly supported the toolbox, including sanctions, and has never argued against their use. At the same time, Belgium has not been particularly vocal in working documents or during its presidency about its eagerness to use the more escalatory measures of the toolbox, what we can find again in the above quote.

Concerning spillovers, we have no cases of spillover from Belgium, in the Belgian presidency priorities however, regarding cyber diplomacy, and its attempts to reorganise the Council working groups, it is noted that: *"the horizontal nature of digital technologies means legislative*

files in this area are often scattered around several working parties, limiting the formation of a consistent approach to digital matters" (Bertuzzi, 2024, p. 1). From the outset, cyber matters touch upon the work of many diverse working groups that would otherwise mainly deal with specific topics. While not a direct result of a specific policy, it is evident here that the establishment of a new working group is being proposed due to the multifaceted nature of cyber matters, which encompass diplomacy as well as economic, trade, security, and other fields. Consequently, cyber diplomacy cannot be separated from the topics it touches upon, creating the need for action in the form of a reorganisation of council working parties.

Bulgaria

Bulgaria is only mentioned once in the analysed corpus and did not participate in the non-papers. However, it has expressed support for the idea of an EU digital diplomacy coordination mechanism led by the Commission and the EEAS (Bertuzzi, 2023, p. 4), which indicates its commitment to Europeanisation and a unified response. This statement was also coded as cross-loading, as Bulgaria seemingly expressed its support alongside other member states in a cross-loading coalition. As this was the only statement we have from Bulgaria, there are no codes regarding uploading or spillover.

Czechia

There are 19 statements from the Czech Republic in the corpus One of which expresses support for autonomy. Czechia has provided feedback and made statements in all the analysed working documents. Therefore, it can be said that Czechia has played an initiative-taking role in the Cyber Diplomacy Toolbox and that this issue is a priority for them, but they did not participate in the non-papers. While some statements have not taken a clear stance on support for the toolbox, many have expressed clear support for Europeanisation and a common approach to cyber diplomacy. Many Czech statements emphasise that work on the Cyber Diplomacy Toolbox must continue and remain a priority for the EU. Notably, Czech support for the toolbox has remained relatively consistent over the years. For example, in 2017 already, Czech comments on WK 2569/2017 INT noted that '*the toolbox should be understood as a set of joint EU responses'* (Council (3), 2017, p. 3), and in 2023 still, Czechia has sought to continue the work on a streamlined unified European response in cyber diplomacy (Bertuzzi, 2023, p. 4)

We can see that substantial cross-loading occurred during the comments on WK 2569/2017 INT in 2017, with nine cases of cross-loading and seven cases of uploading for the Czech Republic. Regarding cross-loading, this mainly concerns references to suggestions made by other member states. Notably, the Czech Republic has referred to German proposals multiple times. *"We agree that the toolbox should mention international law and countermeasures. However, the German proposal in section "Other instruments" is too focused on conduct of individual states. The toolbox should be rather understood as a set of joint EU responses and therefore, we would prefer keeping the original text in place*. (see Council (3), 2017, p. 3) References are made to Portuguese, Slovak and Swedish proposals in other parts of the text (see Council (3), 2017, pp. 2-3). This shows that Czechia was heavily involved in the overall discussion surrounding the proposal. As we have seen before, it is not necessary for a state to support a proposal for it to be counted as cross-loading; acknowledging it and reacting is enough, as the exchange has taken place.

In regard to uploading we also have seven instances in the Czech statements, overall, the Czech proposals of uploading seek to create a more robust toolbox and are in favour of common EU action. Czechia expresses support for some of the more ambitious measures proposed as part of the document: *"We particularly appreciate the following: "..."Emphasis on information sharing, situational awareness and early-warning mechanisms"* (see Council (3), 2017, p. 2).

Czechia also attempted to include stronger wording regarding commitments to adherence to international law (Council, 2021, p. 136). Sometimes, Czechia calls for greater specificity (see Council (3), 2017, p. 2), and in other documents, it supports a more broadly formulated text (see Council, 2021, p. 136). Czechia has also expressed opposition to the politicisation of the toolbox (Council (4), 2017, p. 2), potentially meaning that issues such as incident handling should not be overly politicised, as this could hinder the effective application of the toolbox. Czechia has not made any arguments related to on spillover from other policy fields to legitimate its preferences.

Denmark

Six statements were recorded on behalf of Denmark, in addition to those in the 2018 non-paper, two of which constitute tacit acceptance and all of which provide some form of support for Europeanisation. Denmark has also held a Council presidency during the examined timeframe

in the second half of 2025. In its presidency priorities, Denmark stated its intention to focus further on deterrence and sanctions using the toolbox (Danish Presidency Council of the European Union, 2025, p. 13).

Denmark also joined other member states in formulating the 2018 non-paper on EU cyber restrictive measures. Notably a Danish example is selected to underline in the non-paper, the severity of cyberattacks on the economy: *"Cyber operations are having an economic impact in Europe. For example, the Danish shipping company A.P. Moller-Maersk estimated that malicious activities cost their business USD 200-300m"* (DK/EE/FI/LT/LV/NL/RO/UK non-paper, 2018, p. 1). This is an interesting example of cross-loading and spillover from the economic domain. For one, there is an argument based on national-level economic threat into EU-level external action consequences by supporting the toolbox. At the same time, a cross-loading dynamic is at play, whereby Denmark presumably managed to get its domestic economic threat endorsed as part of the non-paper by the other member states.

For Denmark, two statements are coded with uploading national preferences. In instances where it was difficult to determine whether uploading was involved: Denmark introduced changes to a paragraph in the draft Council conclusions on the EU's cybersecurity strategy for the digital decade (see Council, 2024, p. 24). While most of the changes involve more specific language, they convey the same meaning as the original text and call on the EEAS to specify the actions taken. While the meaning of the text remains largely unchanged, it is unclear whether these preferences stem from a Danish priority. Like Sweden, Denmark has voiced a commitment to further developing the toolbox in this case. In the other instance, as the holder of the presidency, Denmark advocated for further cooperation, notably with the private sector.

Estonia

The corpus includes seven statements by Estonia; however, Estonia was the only member state which was involved in both the 2018 and 2020 non-papers, amounting to another 21 statements as part of these documents, putting it in third place. All the Estonian direct statements favour Europeanisation and in January 2025, Estonia successfully lobbied for the application of the cyber sanctions regime in response to cyber espionage conducted against it in 2020 (Gessant, 2025, p. 1). Estonia also supported the use of the cyber sanctions regime and the toolbox in 2018 in response to attacks against the OPCW (Gessant, 2018, p. 1).

Regarding Estonia's direct statements, there are two cases of cross-loading, and one case of uploading. Notably, as stated above, the EU applied the cyber sanctions regime in 2025 after a cyberattack against Estonia (Gessant, 2025, p. 1). This can be considered a successful uploading of Estonia's national priorities at the EU level, resulting in the entire EU enforcing sanctions against the attackers. Although Estonia has not made any direct statements referencing other member states positions which could be cross-loading, it should be noted however that Estonia participated in both non-papers, as well as a joint call for sanctions with other member states against Russia in reaction to the OPCW cyberattacks (Gessant, 2018, p. 1). In terms of cross-loading, this puts Estonia at the forefront by collaborating with other member states on Cyber Diplomacy Toolbox development and exchanging proposals with each other and serving as a link between the two non-paper author groups. Although Estonia has not made any statements hinting at spillover tendencies, it is worth mentioning again that it participated in two non-papers dealing extensively with spillover.

Finland

For Finland, the corpus includes six statements, all of which express support for Europeanisation. Finland added an emphasis in one of the statements to clearly express support for the creation of the EU Cyber Diplomacy Network (Council, 2021, p. 41), and thus for greater coordination competencies at the EU level. Finland also contributed to the 2018 non-paper, which reinforces the idea that Finland is a proponent of the toolbox and supporter of common action.

Concerning cross-loading, in addition to the cross-loading cases regarding the 2018 non-paper in which Finland participated, Finland has also indicated potential cross-loading in three cases such as by creating an issue coalition with Belgium and Sweden, which were in support of further gradual responses to future cyber attacks (Guarisco, 2018, p. 2). Finland, together with other member states, also wrote a joint letter in 2018 calling for a framework for joint European diplomatic responses to malicious cyber activity (Gessant, 2018, p. 1).

In terms of uploading, Finland has been involved in one case relating to the 2021 draft Council conclusions on the EU's cybersecurity strategy for the digital decade. In this case, Finland sought to include further mention of hybrid threats and disinformation in the text: *"Digital disinformation is clearly on the rise, as seen also during the Covid-19 pandemic. The*

diplomatic toolbox should ultimately also address hacking based disinformation, where the illegality of the hacking would constitute grounds for the use of the diplomatic toolbox" (Council, 2021, p. 41) We can clearly see here that there has been spillover from a different policy realm: the EU's work on preventing disinformation. This is part of the hybrid threats regime. While cyberattacks are often related to hybrid threats and are sometimes considered part of hybrid warfare, the formulation of this quote shows that Finland is arguing based on spillover pressure exerted from outside the cyber diplomacy field. The crux is that hacking-based disinformation would warrant the use of the toolbox, but not other forms of disinformation that do not involve hacking. Finland also explicitly calls for "*further broadening the scope and the use of the Toolbox*" (Council, 2021, p. 41), as a consequence.

France

Having had an active role in the design of the Cyber Diplomacy Toolbox, France has provided us with 22 statements on the subject and was involved in the 2020 non-paper on cyber diplomacy, meaning that we have the second most statements from France. From the perspective of Europeanisation and autonomy, France is an interesting state to examine, as we have 19 Europeanisation codes, as well as two codes as autonomy. This mixture of autonomy and Europeanisation codes is best described as 'cautious Europeanisation'. The two expressions of autonomy are limited to the initial comments from 2017 on WK 2569/2017 INT, the clearest expression being: *"Attribution: we would like to add a sentence saying that attribution is a sovereign decision"* (Council, 2017 (3), p. 16).

This perhaps indicates an initial cautiousness regarding the toolbox, which has since shifted towards a more pro-Europeanisation stance. However, moving on to the Draft Council conclusions on the development of the European Union's cyber posture developed by the French presidency in 2022, it is noticeable that the individual statements contained in the text again seek to avoid infringing upon the established separation of competences between the EU and its member states. This is especially noticeable when we look at the statement: "*REITERATES the importance to strengthen INTCEN's capacity in the cyber domain, based on voluntary intelligence contributions from the Member States and without prejudice to their competences and to explore the proposal on the possible establishment of a Member States' cyber Intelligence working group*" (Council, 2022, p. 13). This statement describes cautious Europeanisation, as it clearly indicates support for Europeanisation by suggesting more EU-

level coordination as part of the working group. At the same time, it pays close attention to avoiding infringement of member state sovereignty by emphasising the voluntary nature of information sharing and the retention of member state competencies. On the same page we also find the statement *"While national security remains the sole responsibility of each Member State"* (Council, 2022, p. 13), which also indicates a similar respect for the agreed separation of competences. In the text, we can also find more explicit support for Europeanisation, for example in the paragraph *"CALLS upon the EEAS, in cooperation with the Commission, to establish by 2023, and update regularly, a list of possible EU joint responses to cyberattacks, including sanction options, across the spectrum in order to be prepared to take swift and effective action when necessary"* here we have a clear preference for Europeanisation and a common response that is at least coordinated by the EU (Council, 2022, p. 14).

Regarding cross-loading and uploading, in addition to the contribution to the 2020 non-paper, France has provided us with two cases of cross-loading and 16 direct cases of uploading. The question of how to interpret the French EU Council Presidency's *draft Council conclusions on the development of the European Union's cyber posture* arose. It is doubtful that the presidency drafted this document alone without input from the EEAS. However, Agence Europe provided the document, stating that the French presidency was the author. Depending on how this document is viewed, France's role in uploading is significantly boosted as this document provided ten statements. While the text does not reference any French domestic priorities or legislation beyond support for the toolbox, French authorship suggests that the priorities set out therein align with the French vision of the toolbox and should therefore be considered an attempt at uploading.

Looking at the proposed policies, France's commitment to intelligence sharing among member states, reinforcement of the toolbox (French Council Presidency, 2022, p. 13) and solidarity among member states (French Council Presidency 2022, pp. 3-4) is evident. Finally, as the presidency, France also calls for *"the Member States and the High Representative, with the support of the Commission, to work towards a revised version of the implementing guidelines of the EU Cyber Diplomacy Toolbox by the end of 2022*" (French Council Presidency, 2022, p. 14). Especially if we look at the comments on WK 2569/2017 INT, France has been very direct in voicing its priorities to be included in the text, one of the clearest cases being the wish to delete the word deterrence from the document regarding the toolbox: *"1/ deterrence : we would*

like to replace all the references to "deterrence" with references to "raising the cost" or equivalent expressions. Deterrence is closely linked with the nuclear business in France and French authorities will not endorse a document where the distinction is not clearly made" (Council, 2017 (3), p. 16). Interestingly, if we look at following documents dealing with cyber diplomacy, the word deterrence continues to be used in this context, and in the French EU Council Presidency Priorities *Draft Council conclusions on the development of the European Union's cyber posture* of 2022 it reads: *"ACKNOWLEDGING that EU declarations and restrictive measures taken in the framework of the EU Cyber Diplomacy Toolbox have sent a strong message that cyber malicious activities targeting the integrity and security of the EU and its Member States are unacceptable and thus contribute to preventing, discouraging, deterring and responding to malicious cyber activities"* (French Council Presidency, 2022, p. 14).

In terms of spillover, if we look at France, we see four cases. This is a special case because the draft Council conclusions on the development of the European Union's cyber posture were produced during the French Council presidency in 2022. This document contains a lengthy section referencing previous EU cyber diplomacy efforts in order to lend legitimacy to the text. The text also references other EU-level policies from related fields (see French Council Presidency, 2022, pp. 3-4). The main focus appears to be on defence and security considerations (French Council Presidency, 2022, p. 3). One such case is the call for intelligence sharing among member states and the establishment of a cyber intelligence working group (French Council Presidency, 2022, p. 13), which is necessary for the effective functioning of the toolbox and constitutes a form of functional spillover. This example illustrates that, for the toolbox to work, member states must take further steps in intelligence sharing. In contrast, France emphasises that the CSIRT network under NIS should under no circumstances seek to establish contact with CSIRTS from third states (Council (3), 2017, p. 16). This clearly indicates pushback against NIS bodies spilling over into the realm of cyber diplomacy.

Germany

The corpus includes 11 statements of Germany, one of which expresses a potential preference for autonomy, Germany was also an author of the 2020 non-paper. Like France, however, we can note a tendency towards cautious Europeanisation in the comments on WK 2569/2017

INT. Germany was not ready to support a common Cyber Diplomacy Toolbox at the European level immediately. *"Germany conceives the reply to the question whether or not the findings of the Issues Paper should be endorsed as Council Conclusions is a function of the substance which Member States will be able to agree. If justified by the contents of such a document, Germany will support its endorsement as Council Conclusions. However, at this juncture the "cyber diplomacy toolbox" still requires amendments; it is at present not ripe for an immediate endorsement"* (Council, 2017 (3), p. 16). However, at no other time in the text does Germany argue based on a preference for the retention of national sovereignty or the status quo. Germany does not rule out the possibility of the toolbox being further developed. Elsewhere in the document, Germany attributes its reluctance to approve the Cyber Diplomacy Toolbox to a lack of precise language. At no point does it express opposition to common action per se(see Council (3) 2017, p. 14). Germanyexplicitly welcomes the pursuit of a joint EU diplomatic response (see Council (3) 2017, p. 14). This is like the behaviour we see from Hungary. The key difference is that Hungary explicitly mentions the separation of powers and member state sovereignty as being potentially under threat (see Council (3), 2017, p. 17).

In 2020, Germany was among the first member states to successfully lobby for the usage of the Cyber Diplomacy Toolbox measures after its establishment in a delayed response to the 2015 Bundestag Hack: *"The EU and Britain imposed sanctions Thursday (22 October) on senior Russian intelligence officers for their alleged role in hacking the computer network in the German parliament in 2015. The head of the GRU military intelligence agency, Igor Kostyukov, and intelligence officer Dmitri Badin have been banned from EU soil and are subject to an asset freeze. A GRU unit, alleged to be responsible for cyber-attacks, has also been added to the EU sanctions list* (Euractiv.com with AFP (2), 2020, p. 1). Germany's lobbying to include the hackers on an EU sanctions list demonstrates its support for a coordinated response among EU member states.

In general, we have seven instances of uploading from Germany, including one of the most straightforward examples of the uploading of a natural priority in the application of the toolbox being argued at EU level. In response to the Bundestag Hack in 2015 and spying on German officials *"the German government will seek in Brussels to use the EU cyber sanctions regime against those responsible for the attack on the German Bundestag"* (Euractiv with AFP (1), 2020, p. 2). This is one of the cases where we can clearly tell that national priorities have

successfully been uploaded to the EU level by applying the toolbox and sanctioning the culprits. Euractiv reports five months later that *"The EU and Britain imposed sanctions Thursday (22 October) on senior Russian intelligence officers for their alleged role in hacking the computer network in the German parliament in 2015"* (Euractiv with AFP (2), 2020, p. 1).

In other instances, Germany pursued uploading as part of the comments on WK 2569/2017 INT. This is evident because other member states reference German proposals and changes. However, it is not possible to code them all since Germany added its proposed changes to the original document in the form of comments and colour codes. These were not visible in the accessible document. Nevertheless, in its more general comments on the document, Germany reiterates the importance of its amendments and would like to see them included in the toolbox (see Council (3), 2017, p. 14).

Another interesting case of uploading is that Germany is supporting the development of the toolbox based on its own China strategy. The reporting on the German Cyber Strategy development states that: "*"Chinese cyber actors [that] are engaged in economic and academic espionage in an attempt to gain access to German corporations' trade and research secrets." Berlin said that it will contribute to the EU Cyber Diplomacy Toolbox, which is currently being revised*" (Hartmann, 2023, p. 4). It is clear here that German support for the toolbox is an expression of its domestic priority to strengthen cybersecurity and economic prosperity. Additionally, while much of the corpus does not mention any non-EU states except Russia, this is the only reference to China in the context of cybersecurity threats.

With regard to cross-loading, Germany has not referenced the proposals of other member states in its own contributions, although it is the state referenced the most by other states, such as the Netherlands (see Council (3), 2017, p. 23) and the Czech Republic (see Council (4), 2017, p. 2), as part of cross-loading. This indicates that Germany played an important role in cross-loading, akin to a cross-loading leader as defined by Aggestam and Bicchi (2019, p. 519).

For Germany, we have evidence of one case that could be considered spillover, in addition to its co-authorship of the 2021 non-paper. There is a suggestion to include the EEAS Hybrid Fusion Cell in cyber diplomacy coordination efforts (Council (3), 2017, p. 4). This is derived from a closely related domain to cyber diplomacy. The German proposal mainly deals with information sharing as part of the Hybrid Fusion Cell in preparation for diplomatic responses.

This is considered spillover although it is already an existing group within the EEAS, as it is call for an expansion of competencies of an EU-body, and there is some 'pressure' being exerted in the German proposal to deepen integration in this regard through coordination at EU-level.

Greece

There is only one mention of Greece in the corpus, alongside other member states. Here, Greece is expressing Europeanisation and cross-loading alongside other member states and arguing for the development of further coordination mechanisms among EU member states (Bertuzzi, 2023, p. 4). However, the overall absence of Greek contributions in other documents leads me to believe that the toolbox was not a particularly salient topic.

Hungary

Overall, Hungary's statements as part of the toolbox discussion were among the most complex. Hungary provided 14 statements on the topic at hand, four of which were coded as autonomy and nine of which mentioned support for Europeanisation, and Hungary was not involved in the non-papers. Similar to Germany, Hungary initially used the narrative of a lack of clarity to justify opposition to the toolbox. However, in contrast to the German proposal, Hungary clearly references the agreed separation of powers and states that unclear language could infringe upon the rights of member states: "U*nder title "Making a decision" the measures which can be "employed by MS in cooperation with the EU institutions or by the EU institutions themselves" must be clearly defined, so that competences based on the EU acquis are respected*" (Council (3), 2017, p. 17).

From this initial statement, the other three statements in which opposition to the toolbox is based on a lack of clarity can also be interpreted as aiming at the retention of member state competencies and opposition to the further enhancement of EU competencies at the time. Similarly, Hungary also opposed some parts of the toolbox proposal due to the ambiguity of the common attribution mechanism (Council (3), 2017, p. 17), which, as previously established, is a particularly sensitive topic for member states as attribution remains a sovereign decision of the member state. Hungary also supports the Council Conclusions, but at the time of writing the opinion, the text was not considered clear enough to be endorsed (see Council (3), 2017, p. 16). Overall, this position is not entirely opposed to further Europeanisation, provided that the competencies and rights of the member states are respected. Hungary does

not oppose further Europeanisation as part of the draft Council conclusions on the EU's cybersecurity strategy for the digital decade. During the Hungarian Council presidency in 2024, Hungary also refers to the development of common EU standpoints in digital diplomacy for multilateral forums and the continuation of cyber diplomacy outreach, especially in the Balkans (see the Hungarian Presidency of the Council of the European Union, 2024, pp. 38-39).

Regarding cross-loading, Hungary has not participated in the drafting of the non-papers and has only referenced the position of one other country. Therefore, Hungary is considered to have engaged in cross-loading only in two occasions. An example of this is the Hungarian Council Presidency's reference to the digital diplomacy work of the previous Belgian Council Presidency, indicating that Hungary would continue the previous efforts (Hungarian Presidency Council of the European Union, 2024, p. 38).

If we look at uploading, Hungary was more active with a total of nine cases of uploading. Hungary (see Council (3), 2017, p. 4), has pursued inclusion of the OSCE and its efforts in the realm of cyber confidence building measures in the 2017 comments on WK 2569/2017 INT: "*As we have stated during the Horizontal Working Party on Cyber Issues of 22 March, we think that the work done in the OSCE on cyber Confidence Building Measures should feature more prominently in the document. Every EU Member State is also a participating State in the OSCE. The OSCE has adopted 16 confidence building measures, some of which could also be referenced in the cyber toolbox. The OSCE Informal Working Group dealing with cyber issues will concentrate in 2017 on the implementation and operationalization of these Confidence Building Measures, which could eventually be also useful in the context of the diplomatic toolbox, like for example the consultation mechanism under CBM3"* (Council (3), 2017, p. 16). As explained previously, Hungary sought to include more sovereignty-related sentences in the 2017 document, such as the quote concerning respect for acquis competencies between the EU and member states. (Council (3), 2017, p. 17).

Examining Hungary's suggested changes to the 2021 Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade reveals a double nature. On the one hand, the changes express support for joint action (see Council, 2021, p. 65). However, they also emphasise the need for deliberation within the Council on all activities related to the toolbox, particularly the preparatory processes for decisions (Council, 2021, p. 65), as well as discussions on the EEAS's activities in this area (Council, 2021, p. 66). Although they express

support for joint action at EU level, the changes also indicate a reluctance to allow the EEAS to act independently of supervision by member states, as well as an adherence to the principle of obtaining the approval of all member states before pursuing toolbox measures. Tracing back to Hungary's priorities for the 2024 Council Presidency, they include increased intelligence sharing among EU member states and capacity building in its immediate neighbourhood, the Western Balkans (Hungarian Presidency Council of the European Union, 2024, p. 39). For Hungary there are no codes of spillover.

Ireland

Of the four statements from Ireland in the table, two are coded as tacit acceptance. Overall, there are no statements in favour of autonomy, and three indicating support for common action. The coding of the Irish active statement on the draft Council conclusions on the EU's cybersecurity strategy for the digital decade was also particularly challenging. Initially, it was coded as autonomy because Ireland added a comment supporting more agreed language and the removal of the more ambitious language used in the paragraph. They also supported the removal of cooperation with NATO and the insertion of text relating to an increased EU-UK-US relationship in cyber diplomacy (see Council, 2021, p. 74). However, on reflection, the Irish comments do not relate as much to the issues of autonomy and a common response, nor do they argue for the retention of member state sovereignty. As the paragraph as a whole does support the development of a toolbox, it was coded as Europeanisation.

It is also worth noting that Ireland did not advocate the use of the toolbox when it was the victim of a cyberattack in 2021 (see Gessant, 2021, p. 1; see also Sachs et al., 2024, p. 18). At the same time, Poland, which was also affected, requested the use of the toolbox. Also, Ireland did not participate in any non-papers, these can also be seen as indicators of a certain hesitance from Ireland towards the toolbox.

Regarding uploading, two statements have been coded as such. Ireland is engaged in one of the clearest cases of uploading as part of the draft Council conclusions on the EU's cybersecurity strategy for the digital decade. As mentioned above, Ireland has sought the removal of the mention of NATO (see Council, 2021, p. 75). As a neutral country, this seems to be in line with Ireland's national priority of maintaining its neutrality. An interesting note on page 74 refers to a previous reference to NATO: "*Reference to NATO removed in accordance with the*

Presidency's email of 4 February". Without access to the email, we can only speculate about its contents. However, judging by the changes made by Ireland to the document, as well as that Ireland was the only state to address this change, it can be assumed that the change to the mention of NATO was in line with their priorities.

On the other hand, we have Ireland seeking more inclusion of cooperation with the US and UK in the text in matters of non-military cooperation, especially trade with the UK "*Ireland strongly supports a reference to the transatlantic relationship but this should not be limited (as was the case in paragraph 27) to the context of threat landscape and responses. Furthermore, Ireland wishes to see a reference to the EU UK TCA*" (Council, 2021, p. 75), reminiscent of the important relationship Ireland has with these countries.

Ireland has also been attentive to the use of agreed language when it comes to restrictive measures (see Council, 2021, p. 74), as demonstrated by its decision not to call for the use of the toolbox when its national health service was the victim of an attack (see Gessant, 2021, p. 1) (see Sachs et. Al. 2024, p. 18). This might reasonably suggest that Ireland is seeking to adopt a less confrontational attitude towards the toolbox usage, in contrast to the more security-deterrence oriented language seen from some other member states.

In terms of spillover, there is one ambiguous case from Ireland: the argument based on the EU-UK Trade and Cooperation Agreement. Although this falls under a different domain to cyber diplomacy, the quote highlights the importance of the document's paragraphs dealing with cyber dialogue and cooperation provisions. However, as there is a clear link between the economic rationale and trade policy and cyber diplomacy in this case, it was counted as spillover. The reason for doubting whether this constitutes spillover is that Ireland is not primarily basing itself on trade, but on the cyber-related articles belonging to a very broad agreement that is inherently interlinked with many other EEAS diplomatic initiatives, including cyber diplomacy. Nevertheless, there is an argument to be made that this is spillover, since while another EU policy document is clearly referenced, it links to existing cyber diplomacy measures and calls for the toolbox of cyber diplomacy measures to be expanded, as well as the Trade and Cooperation Treaty to play a more important role by linking it to cyber security. At the same time, it is Ireland's domestic preference that leads to the mention of these articles.

Italy

Italy was already identified by Ivan (2019, p. 7) as one of the more cautious member states regarding the Europeanisation of the Cyber Diplomacy Toolbox. This was also found to be the case, especially when considering the news correspondence: nine of the Italian statements were coded as advocating for autonomy and two were supportive of Europeanisation, Italy did not participate in the non-papers. Italy is also notable because it is the member state that has been the subject of the most news articles; therefore, we have 11 statements concerning Italy in the corpus. This is because Italy opposed further sanctions against Russia as part of the cyber sanctions regime: *"Italy is resisting a European Union push to impose sanctions on states who carry out cyberattacks, a move that appears in line with Rome's calls to de-escalate tensions with Russia but that could alienate Italy from its EU allies."* (Guarisco, 2018, p. 1)

This clear opposition to further Europeanisation regarding the toolbox and the cyber sanctions regime indicates Italy's support for retaining autonomy in matters of cyber diplomacy and cyber sanctions, as it views the prospect of common European action as detrimental to its own foreign policy goals. While this can be perceived as a national priority, news sources cite the close relationship between Italian Minister Salvini and Russian President Putin as a catalyst for this opposition (see Brzozowski, 2018, p. 2).

However, opposition to increasing Europeanisation continues beyond 2018, as evidenced by the Italian comments on the 2021 Draft Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade. Italy has made multiple changes that considerably soften the text's commitment, for example by deleting the more constraining language regarding the establishment of an EU Cyber Intelligence Working Group: *"While national security remains the sole responsibility of each Member State, ACKNOWLEDGES the importance of strategic intelligence cooperation on cyber threats and activities, and INVITES Member States, through their competent authorities, to continue to contribute to EU INTCEN's work, including by exploring the ~~establishment~~* ***benefits and possible mechanisms*** *of an EU Cyber Intelligence Working Group"* (Council 2021 p. 82). Italy goes on to remove the following sentence from the text: ~~*"WELCOMES the establishment of an informal EU Cyber Diplomacy Network by the High Representative for Foreign Affairs and Security Policy with a view to developing the engagement and expertise of both EU delegations and MS embassies on international cyber issues in order to strengthen coordinated outreach."*~~ (see Council, 2021, p. 82). This was

interpreted as a clear indication of opposition to joint action and further Europeanisation regarding cyber diplomacy.

The two positive mentions of Europeanisation in Italy's statements were coded as tacit acceptance, indicating that no concrete opposition was expressed to the paragraphs dealing with cyber diplomacy. However, paragraph 24 of the document takes special care to ensure that national competencies are not infringed upon, which could help to explain why there was no opposition to this part of the text (see Council, 2021, p. 82). Overall, from what we see in the corpus, it is confirmed that Italy favors autonomy in matters of cyber sanctions and the Cyber Diplomacy Toolbox.

Regarding cross-loading and uploading, Italy is again a special case because it depends partially on how the news articles are interpreted. We have three codes of uploading from Italy, and none regarding cross-loading. One instance has been coded as uploading rather than cross-loading. To understand why, we must reconsider the criteria that constitute cross-loading in the coding scheme: the attempted exchange of information with other member states outside of a formal EU context. So far, cross-loading has only been coded in cases where references were specifically made to other member states or where there were collaborative efforts by groups of member states. *"Italy has repeatedly urged a relaxation of the sanctions against Russia, which has been the target of a wide range of EU economic penalties since the 2014 Ukraine crisis"* (Guarisco 2018, p. 1), the issue in this case was to determine who is being urged. As Italy is unilaterally urging this change, which would probably take place at the EU level, where the common cyber sanctions mechanism is settled, this would be more akin to an attempt to upload a national priority to the EU level. In this case, it would involve uploading an autonomy-sovereignty discourse by halting the toolbox altogether. This is in line with the cases of uploading from the draft Council conclusions on the EU's cybersecurity strategy for the digital decade. In both cases, Italy uploaded a sovereignty-autonomy statement. Of particular importance is the deletion of the paragraph on page 82 of the document (see Council, 2021), which was cited above already. Here, rather than adding a statement, a paragraph is deleted. This could be termed 'negative uploading', whereby a national priority is uploaded through the means of deletion. The last instance of uploading for Italy, also cited above on this page (Council, 2021, p. 82), where *'establishment'* is replaced with *'benefits and possible mechanisms'* which also supports the autonomy discourse. There are no quotes by Italy that would express spillover.

Latvia

Overall, we have 11 statements from Latvia and Latvia also participated in the 2018 non-paper. Three of the comments are coded as autonomy, while in all the other comments made regarding the topic of WK 2569/2017 INT, clear support for Europeanisation is evident. Latvia made the following comment on a paragraph dealing with attribution of cyberattacks: *"We will not solve all attribution issues here. Either have all issues here or split a simplified toolbox and invest in a longer paper on international law and attribution separately. b. Attribution will also be case by case always. Cannot be codified here"* (Council (3), 2017, p. 18). This paragraph fulfils some of the criteria for autonomy by making attribution a case-by-case issue that does not always require a common European response. Rather, the paragraph argues that attribution should not be codified at the European level therefore one could interpret this statement as an expression of autonomy. However, the argument based on the broader context is not that Latvia wishes to maintain its sovereignty, as we have seen in the Italian case, rather, the argument is based on the idea that as many member states as possible can reach consensus on the text. Ultimately, the aim is to achieve unanimous approval of the text and pursue Europeanisation. *"We support brief council conclusions addressing the need for a common EU approach on a joint diplomatic response to cyber operations. A high level message on the threat faced by the EU is an appropriate first step in addressing an initial diplomatic response. More detailed and challenging issues addressed in document WK 2569/2017 INIT that can be further elaborated in a document in the future or even within the context of an EU Cyber Security Strategy review".* Overall, Latvia expressed more support for Europeanisation but was willing to compromise on the more challenging aspects of the text to ensure a united European approach, with a view to achieving more ambitious Europeanisation in the future. Some of Latvia's comments from 2021 regarding the cyber posture also adopt a similar stance. In addition to contributing to the 2018 non-paper, Latvia has issued two cross-loading statements. Alongside other member states, Latvia has expressed support for sanctions against Russia in response to OPCW cyberattacks (Gessant, 2018, p. 1).

Regarding uploading, Latvia provided us with several interesting statements in 2017. Latvia expressed a preference to include hybrid threats in the text and called for NATO to be included in comments on WK 2569/2017 INT (see Council (3), 2017, p. 18). Moving on to the draft Council conclusions on the EU's cybersecurity strategy for the digital decade of 2021, Latvia again underlined NATO's importance in the text (Council, 2021, p. 91). At the EU level, Latvia

has expressed its willingness to include the CSIRT network of the NIS Directive in the toolbox for application, information sharing and attribution (see Council (3), 2017, p. 18).

Latvia is also an interesting case when we look at spillover, we have three examples of spillover in Latvian statements, all stemming from the comments on WK 2569/2017 INT. On page 18 of the document, Latvia refers to the role of EU frameworks such as ENISA and the CSIRT network, especially in the context of the NIS Directive (Council (3), 2017, p. 18). This direct reference to institutions and bodies of the NIS Directive constitutes spillover, as it would grant them a direct expansion of competencies beyond their strict domain of cybersecurity management into cyber diplomacy. Latvia's main rationale for the spillover is that cyber diplomacy is also an economic concern (Council (3), 2017, p. 18), and therefore these bodies should be involved, here economic considerations are creating direct pressure to deepen integration.

Lithuania

We have six statements by Lithuania, as well as its participation alongside other member states in the 2018 non-paper. All direct Lithuanian statements express support for Europeanisation. Regarding Europeanisation and autonomy, Lithuania appears to adopt a similar pro-Europeanisation stance to Latvia, and establishing a common EU position is a priority: *"Implementation of the EU Cyber diplomacy toolbox and its measures is of utmost importance, respectively, we suggest to underline restrictive measures aim following the agreed language across various CCs and Declarations"* (Council, 2021, p. 98). Lithuania also pays specific attention to the importance of the deterring factor of the toolbox mechanisms (see Council, 2021, p. 98).

For Lithuania, we have three statements indicating cross-loading and two indicating uploading, the latter are taken from the draft Council conclusions on the EU's cybersecurity strategy for the digital decade. One of these mentions the explicit inclusion and emphasis on restrictive measures by Lithuania (see Council, 2025, p. 98), which is consistent with the Lithuanian stance that deterrence is of fundamental importance. Lithuania also includes an example of uploading alongside tacit acceptance in paragraph 26, in which Lithuania moves NATO further ahead in the list of relevant international organisations to emphasise its importance, rather than adding or removing words. This demonstrates that uploading and expressing preference can

also involve shifting words if there is meaning behind it: *"Recalling EU-NATO Joint Declarations and its strategic partnership, it is important to mention NATO after the UN"* (Council, 2021, p. 99). There is no spillover code except for its non-paper participation.

Malta

We have three statements from Malta in the corpus, all of which express support for a joint approach but two of which are marked as tacit acceptance. Malta did not participate in the drafting of the non-papers. Overall, Malta did not have strong preferences regarding the toolbox, as there are only statements included from the 2021 Cyber Posture but at least tacitly supported a common European response. One of the statements was coded as relating to the Maltese insertion of economic security in paragraph 26 of the document (see Council, 2021, pp. 107-108), which could potentially reflect a domestic policy priority by Malta. The mention of *"our economic security"* (Council, 2021, pp. 107-108) also constitutes a spillover, arguing for the need for an effective Cyber Diplomacy Toolbox and the usage of all CFSP measures to ensure the EU's safety through the importance of deterrence to ensure economic security.

Netherlands

The Netherlands is the member state for which we have the most content in the dataset. As the presidency that first proposed the toolbox the Netherlands were able to keep going with the agenda of the toolbox development over the years of development. We have a total of 31 statements of the Netherlands, as well as its contribution to the 2018 non-paper along with other member states. For the Netherlands, we also have very mixed results when it comes to common action and autonomy, 15 times common action and Europeanisation was mentioned positively, but also eight times autonomy was preferred, the rest of the time no concrete preference was articulated. It is important to repeat that the Dutch Presidency in 2016 published the initial non-paper supporting the development of a Cyber Diplomacy Toolbox, hence why it must be underlined that the Netherlands has positioned itself from the start as one of the primary proponents of common action.

Like what we have seen with Latvia, some of the Netherlands's statements take a stance favouring autonomy, even when the overall direction of most statements indicates a preference for common action. In the comments on WK 2569/2017 INT, the Netherlands takes a clear stance favouring sovereignty when it comes to the issue of attribution, choosing to clearly

differentiate between legal and technical attribution of cyberattacks (see Council (3), 2017, p. 23) but also adding that: *"NL considers it important to take the fact that attribution is primarily a sovereign national decision by Member States as the point of departure for these considerations"* (Council (3), 2017, p. 23). Also, the Netherlands underlines that information sharing is primarily the responsibility of the member states, who should determine what information they wish to share (see Council (3), 2017, p. 23). Throughout the text, there are also multiple suggestions to change the wording to make it less legally constraining. Interestingly, this repeatedly applies to mentions of respect for international law (see Council (4), 2017, p. 5).

In a different paragraph, the Netherlands expressed strong opposition to the use of the EU's CSIRT network to contact states outside the EU (see Council (3), 2017, p. 19). This was a difficult case to code as it simultaneously supports common action and information sharing among member states while also placing member states at the centre of this activity as the primary actors, both within CSIRT actors and in relation to non-EU CSIRTs, who should primarily use bilateral exchanges with EU member states. Due to the primacy given to the bilateral relations that member states have with outside states, this was coded as autonomy. Conversely, in the same comments, there are also some strong indications of support for Europeanisation; one of the most straightforward being: *"NL is in favor of moving forward with the Council Conclusions as soon as possible in order to provide a political signal to (potential) malicious actors*" (Council (3), 2017 p. 19)

As the presidency during the initial development of the toolbox, the Netherlands naturally took on the role of promoting its development. At the same time, as we have seen in the Latvian case, it is important not to move too quickly towards a common response for fear of alienating other member states. Therefore, the Netherlands had to propose a common response in some fields while ensuring that existing member state sovereignty and agreed competencies are not violated. We find proof of this in the paragraph: *"STRESSING THAT many of the measures belonging to such a Toolbox do not always require public attribution to a State or non-State actor, and can be used to exert political pressure without making direct accusations by the EU and its MEMBER STATES"* (Council (4), 2017 p. 5). It is emphasised here that member states do not automatically attribute attacks using the toolbox. This is in line with the agreement that

attribution is a sovereign decision. At the same time, it seems as if this paragraph serves to enable easier consensus on common attribution among Council members.

Examining the applications of the toolbox reveals that the Netherlands has consistently advocated for and supported the policy and common action post-2017. In 2018 and 2022, Dutch information sharing and Dutch domestic interests have consistently advocated for the use of the toolbox (see Leeson, 2022, p. 1) (see Brzozowski, 2018, p. 1) which is an indicator of support for a common European response.

As an initiator of the toolbox, the Netherlands again occupies a special position with regard to uploading, 21 statements were coded as uploading. The Netherlands has shown ambition in integrating international law into the text when it comes to uploading (see Council, 2017, pp. 21-22). However, it could be argued that international law cannot be uploaded since it is already above European law, to which the EU is already bound. From these examples, we come to understand that the Netherlands does not simply upload international law to the toolbox, but rather its own interpretation and application of it. As we have seen with Austria, there is also a national priority to abide by international law. The will to adhere to international law constitutes a policy preference in and of itself. We can see that the Netherlands has a distinct understanding of the role of the toolbox and how it relates to provisions of international law: "*NL would suggest that this paragraph should not be narrowed to actions that are available in response to an internationally wrongful act (such as countermeasures under the law of state responsibility). This paragraph should be expanded to actions that can be undertaken in response to cyber operations that constitute an unfriendly act in general (such as expulsing foreign diplomats)*" (Council (3), 2017, p. 22).

The Netherlands also show that support for the toolbox can be uploading due to the alignment of preferences between toolbox goals and member states interest, where their domestic interest is directly served by having a strong toolbox: "*An option for taking the implementation guidelines forward would be to include these as an action in the roadmap of the EU cyber security strategy as it is updated. This would be in line with the Dutch view on strongly featuring international engagement, diplomatic relations, political-strategic aspects and capacity building in the second EU cyber security strategy*" (Council (3), 2017, p. 19).

Regarding the Netherlands, there is also a strong case for uploading national priorities regarding the application of the toolbox to the EU level. This is in response to the Dutch government's call to sanction Russian hackers: "*Ruling party VVD wants Russian hackers added to the EU's list of sanctioned people to ensure they lose access to their financial accounts in Europe. "They are hackers who daily attack companies in the Netherlands, our small and medium-sized enterprises…*" (Leeson, 2022, p. 1). Here, we can clearly see a national preference being attempted at the EU level. Of interest in this regard is the mention of Europe as a geographical area: As soon as the hackers are added to the list, "*we can grab them if even one wheel of their fat Lamborghini enters a European country," the VVD MP also said*" (Leeson, 2022, p. 1). The domestic preference and perceived threat to the Netherlands is being enforced through common European action, beyond Dutch borders, a typical case of the megaphone in CFSP.

The Netherlands has also engaged in uploading autonomy narratives in some cases, as we have seen above (see Council (3), 2017, p. 19) (see Council (3), 2017, p. 23), where the text was often tweaked only slightly, with the same meaning largely prevailing but with a less constraining character. One such case is changing '*abide by*' to '*respect*' (Council (4), 2017, p. 6), indicating a lower level of adherence. These tweaks may also be based on previously agreed EU language.

The Netherlands played an important role in cross-loading, with eight cases, often referring to the German comments on WK 2569/2017 INT multiple times (Council (3), 2017, p. 23). The Netherlands was also identified as one of the states with the capacity to conduct serious cyber forensics and share this information with other member states, as demonstrated during preparations for foreign cyber interference in the European elections. Along with the UK (which was still in the EU at the time) and the US, the Netherlands publicly criticised Russia for its malicious cyber activities (Brzozowski, 2018, p. 2), which presumably influenced other member states to support sanctions. This also illustrates that member states may pursue unilateral action, or act together with actors outside the EU when their interests are not met.

Finally, regarding spillover, it is notable that the Netherlands has not used spillover narratives more actively to advocate for additional EU competencies. In fact, most of the Netherlands' arguments and contributions are statements of preference that are generally not based on spillover from other policy areas. The only mention of spillover is the call for the further

development of the Cyber Diplomacy Toolbox implementation guidelines as part of another policy document, the EU cyber security strategy (see Council, 2017, p. 19). However, given that this is merely a reference to another EU policy document and a potential expansion of its scope, it can hardly be considered a significant expansion of competencies. Like France, the Netherlands has also opposed the CSIRT network taking on a role in cyber diplomacy with third states (see Council (3), 2017, p. 19).

Poland

There are four statements from Poland, as well as the contributions to the 2020 non-paper. Three of these support common action and Europeanisation. There is little information on Poland's stance during the initial development of the toolbox, but Poland supported the use of the toolbox in 2018, alongside other member states (see Guarisco, 2018, p. 2), and advocated for its use in response to Russian cyberattacks against it in 2021 (see Gessant, 2021, p. 1), which is coded as an expression of support for common action. Considered together with the overall positive attitude towards Europeanisation, expressed as part of the 2020 non-paper, it can be said that Poland has moved towards being an advocate of common action.

We have two statements indicating uploading from Poland, and three cases of cross-loading. Concerning uploading, regarding the cyberattacks against Poland and Ireland in 2021, the Polish Prime Minister, Mateusz Morawiecki, said: "*Cyber attacks from Russian territory must cease immediately. We have proof that these attacks were aimed at destabilising, spreading disinformation and weakening the whole of the EU*" (Gessant, 2021, p. 1). This cannot be considered uploading alone because there has been no concrete attempt to influence European-level policy based on a Polish national preference; rather, action is being called for from Russia. However, further on in the text, it states that: '*In their conclusions, the leaders invite the Council to "explore appropriate measures within the framework of the cyber diplomacy toolbox"* (Gessant, 2021, p. 1). As suggested by the reading of the article, here the leaders of EU member states that make up the Council, are collectively acting upon the Polish call for action, and therefore qualifies as uploading. For Poland, we do not have indications of spillover except for what is included in the non-paper.

Portugal

In total, we have six statements from Portugal, all of which indicate support for Europeanisation and a common response, Portugal also contributed to the 2020 non-paper. Having held a council presidency during the period of the study, Portugal played an important role in trying to increase the effectiveness of the toolbox, particularly by developing punitive measures and seeking to strengthen mutual assistance and coordination among member states. This was achieved by developing links between the toolbox and existing EU-level legislation in this area (see Stolton, 2021, p. 1-2). As early as 2017, Portugal called for increased coordination and a stronger role for EU institutions in managing member state efforts, as well as expressing clear support for common responses: *"Cyber malicious activity has thus become the weapon of choice in strategic confrontation below the threshold of armed conflict. Consequently showing determination at the highest political level to use the whole range of EU and national diplomatic tools, to respond collectively to cyber attacks against MS, is crucial" ... "the Council should nevertheless give a clear mandate to the EEAS to conceive, plan and coordinate joint cyber diplomacy exercises encompassing the cyber policy teams of the ministries of Foreign Affairs of MS"* (Council (3), 2017, p. 25).

From Portugal, we have two cases of uploading and two cases of cross-loading. Portugal held a Council presidency in 2021, during which it sought to influence the Cyber Diplomacy Toolbox in combination with other EU mutual assistance mechanisms (see Stolton, 2021, pp. 1-2). Portugal sought to upload its own priority of creating a stronger toolbox and gave the EEAS a mandate in 2017 (see Council (3), 2017, p. 25). Regarding cross-loading, Portugal has circulated a discussion paper independently on strengthening EU coordination regarding digital diplomacy in view of coordination at the UN. This is a clear example of Portugal trying to influence other member states to support its proposal (Bertuzzi, 2023, p. 2).

We also have two cases of spillover from Portugal. On the one hand, linking Portugal to the extension of punitive measures that form part of the Cyber Diplomacy Toolbox, as well as to existing EU legal mechanisms, could be considered spillover. This is because it represents an expansion in the applicability of previous EU law, based on threats from cyber and terrorist attacks (see Stolton, 2021, pp. 1-2). Secondly, Portugal has clearly stated its intention to further develop the toolbox in response to threats to supply chains, critical infrastructure and essential

services, which could be viewed as an economic and security rationale (see Stolton, 2021, p. 1).

Romania

The corpus includes six statements by Romania all of which support Europeanisation, of which three were coded as tacit acceptance. Romania participated in the drafting of the 2018 non-paper. Romania also had a Council presidency in 2019 which put it in a good position to further pursue Europeanisation and common response. Romania raised no objection to the *Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade*'s paragraphs dealing with the toolbox and accepting these paragraphs that generally call for a common European response and further development of EU-level consultation mechanisms such as the EU Cyber Diplomacy Network (Council, 2021, p. 116). During the Romanian presidency, it is reported that one of the presidency's goals was to have the cyber penalty regime passed during their term in office (see Gessant, 2019, p. 1). This clearly indicates support for a common response.

Considering uploading and cross-loading, Romania has not made any direct uploading attempts in the examined corpus. In addition to the participation in the 2018 non-paper, Romania has participated in a cross-loading coalition together with other member states calling for application of the toolbox (Gessant, 2018, p. 1) (Guarisco, 2018, p. 2). Romania has also not made direct spillover references beyond what is contained in the non-paper.

Slovakia

The corpus includes nine statements from Slovakia, six of which support common action, while two are coded as supporting autonomy. The statements derived from the comments on WK 2569/2017 INT were difficult to code for Slovakia because comments made by Slovakia were not clearly marked as such in the text. Furthermore, as the original draft was not accessible on which Slovakia based its comments, which statements were Slovak and which were made by the EU and left unchanged could not be discerned, which would have constituted tacit acceptance. Nevertheless, all the statements in that document should be considered in line with Slovak priorities. The Slovak paragraphs generally express support for *"the firm governance and coordination of the EU cyber policy with clear competences, roles and tasks, either strategic or operational, across the EU institutions, agencies and other bodies "(*Council (4),

2017, p. 9). Slovakia also recognises the role of the NIS directive bodies in coordinating cybersecurity threats (Council (3), 2017, p. 9).

On the other hand, two of the statements may suggest an initial reluctance to pursue full Europeanisation. Notably, Slovakia deleted a reference to ~~*the framework of effective policy coordination*~~ from a paragraph (Council (4) 2017, p. 9) and changed the wording from "*WELCOMING the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications"* as it was in the Dutch paragraphs to *TAKING NOTE* (see Council (4), 2017, p. 9). The deletion of the sentence indicated to me a reluctance to enshrine formal coordination duties in the text, and the change in wording regarding the UN recommendations suggested opposition to making them binding. As this is an area where the spheres of the EU and the UN overlap as part of an EU draft, I have chosen to code it as an expression of autonomy, even though it initially comes from the UN level, it still presents a European commitment in this case. However, this contradicts Slovakia's generally pro-European stance elsewhere in the text, as well as its support for the joint sanctions imposed on Russia in 2018 (see Gessant, 2018, p. 2). For this reason, Slovakia would still be classified as a supporter of joint action at the time.

If we look at uploading and cross-loading from Slovakia, we must essentially look at the comments on WK 2569/2017 INT. Here we have two cases of cross-loading and six cases of uploading. As previously mentioned, Slovakia has changed some of the language in the paragraphs to less constraining language (see Council (4), 2017, p. 7). On page 9 of the document, Slovakia added two paragraphs compared to the original. One of these calls for clear delineation of tasks and competencies between the EU IBAs to ensure that the toolbox functions properly and achieves its goals (see Council (4), 2017, p. 9). Slovakia also introduced an entirely new paragraph, making clear mention of cooperation and coordination in the response to large scale cyber incidents, especially in view of "*the revised EU Cyber Security Strategy, while recognising the role of the NIS Directive bodies*" (Council (4), 2017, p. 9). This paragraph highlights the need for effective coordination and a functional toolbox, indicating a heightened priority. At the same time, this constitutes the only code of spillover from Slovakia, as there is a clear reference to the importance of the NIS Directive, which calls for further coordination at the EU level in the revised EU Cyber Security Strategy. This could potentially expand the competencies of NIS bodies into cyber diplomacy.

Slovenia

From Slovenia there are no direct statements, but Slovenia has participated in the drafting of the 2020 non-paper. Judging by the contents of the non-paper, Slovenia is an overall proponent of the toolbox, but not a particularly active one. Similarly, except for cooperation on non-papers, we have no direct case of up- or cross-loading or spillover from Slovenia.

Spain

The table includes four statements from Spain, three of which are coded as tacit acceptance. All of these were coded as Europeanisation. The fact that we only have statements from Spain coded as tacit acceptance of the paragraphs dealing with the Cyber Diplomacy Toolbox does express support for the Europeanist ideas contained therein but also suggests that the toolbox was not the biggest priority at the time. We also have an explicit mention of Spain in relation to a digital diplomacy coordination mechanism among EU member states (see Bertuzzi, 2023, p. 4), which supports the idea that Spain positioned itself as a supporter of further Europeanisation and a common response. There are no statements coded as uploading or as spillover from Spain in the corpus, but one statement coded as cross-loading when it acted together with other member states to support a coordination mechanism (Bertuzzi, 2023, p. 4)

Sweden

In total the corpus includes 14 statements from Sweden. Sweden has expressed autonomy in three cases, and support for Europeanisation in nine. Two statements supporting autonomy stem from the comments on WK 2569/2017 INT and underline the primacy of member states and their sovereignty, especially in matters of attribution: *"Conclusions should firmly stress that a decision to attribute is the sovereign responsibility of the individual Member State, on the basis of its individual political and legal assessment"* (Council (3), 2017, p. 27). The other two connected items were less nuanced in their expression. They called for certain fields to be included in future documents for analysis, such as the process for initiating joint action and the use of restrictive measures with other Member States (see Council (3), 2017, p. 27). It is important to note that in both cases Sweden specifically mentioned the need for individual attribution by member states (see Council (3), 2017, p. 27). Sweden did not explicitly state its support for these measures, but rather their analysis. This is why it is coded as predominantly supporting autonomy. *"Conclusions should include a follow up and way forward clause,*

indicating the areas where further work and analysis will be needed" (Council (3), 2017, p. 27). This should be classified as a case of cautious Europeanisation as we have seen before in relation to this document, which was novel in 2017, where member states were still careful not to be too ambitious in the development of the toolbox and not to infringe on established competencies.

On the other hand, other statements made by Sweden in 2017 clearly support common action by arguing in favor of information sharing and coordination among member states, such as: *"Conclusions should stress the need to make full use of existing mechanisms for joint situational awareness and exchange of information. Also including exchange of information between EU and NATO"* (Council (3), 2017, p. 27) Integration of such way-forward clauses is something we see again from Sweden four years later in the comments on the EUs cyber posture (see Council, 2021, p. 131). Like what we saw with Latvia, we also see Sweden taking a stance where the issue of attribution is being circumvented, probably with the aim of ensuring the toolbox is passed and that common response can be applied (Council (3), 2017, p.27).

Sweden also held the Council of the European Union presidency in the first half of 2023. In its priority paper, it explicitly mentions cyber diplomacy and digital diplomacy efforts, as well as the pursuit thereof, to play a bigger part in European external action. It also mentions the strengthening of the sanctions regime which signifies support for a common response (Swedish Presidency of the Council of the European Union, 2023, p. 7).

Nine statements are coded with uploading and one with cross-loading for Sweden. Regarding uploading, Sweden has made rather nuanced suggestions. A core feature of the Swedish proposals is the clear distinction between 'could' and 'should' statements concerning uploading; the latter clearly express a stronger preference. Sweden has made suggestions regarding the design of the Conclusions to be adopted, as part of the comments on WK 2569/2017 INT. These include a preference for information exchange, presumably within the Council but also between the EU and NATO (Council (3), 2017, p. 27), as well as emphasising the importance of international law and measures that do not require attribution (Council (3), 2017, p. 27). Sweden has also supported the integration of text that clearly expresses respect for the sovereignty of member states to attribute (Council (3), 2017, p. 27). Notably, Sweden included a way forward clause in the text (Council (3), 2017, p. 27), indicating that the further development of an effective toolbox is a Swedish priority. Regarding the draft Council

conclusions on the EU's cybersecurity strategy for the digital decade, Sweden has made substantial changes to paragraph 23. Some of these are mere language adjustments, but interestingly, Sweden has also reintroduced the possibility of a way-forward clause (Council, 2021, p. 131), indicating that the development of the toolbox is Swedish priority pursued at EU level.

Looking at the Swedish Council priorities, here Sweden pledges that it will "*work to implement and develop the EU's response to antagonistic cyber threats*" (Swedish Presidency of the Council of the European Union, 2023, p. 7). It also prioritises cyber diplomacy as part of EU foreign policy, stating that: '*Sweden will work to better integrate cyber diplomacy issues and the EU's external digital policy into its overall foreign policy*' (Swedish Presidency of the Council of the European Union, 2023, p. 7). The issue here is that the quote is imprecise in terms of which foreign policy is meant. On the one hand, it could mean that Swedish foreign policy is being influenced by the EU level, which would indicate downloading. However, I interpret it as meaning that Sweden is advancing these priorities as part of European foreign policy based on its own priorities for European cyber diplomacy and digital policy. This constitutes priority-setting based on national preferences and therefore uploading.

With regard to spillover, there are two cases from Sweden on page 26 of the comments on WK 2569/2017 INT. Firstly, Sweden argues that the Council conclusions should be based on the EU's security and foreign policy goals in order to justify the development of the EU's cyber diplomacy tools (see Council (3), 2017, p. 26). Secondly, Sweden emphasises the importance of linking the EU's security interests in ensuring the free flow of information and economic growth to the development of the toolbox and its measures (see Council (3), 2017, p. 26). This demonstrates spillover from the fields of defence and the economy, which validates the EU's further competencies in the cyber diplomacy domain.

UK

From the perspective of the autonomy-Europeanisation axis, the UK is an interesting case because it left the EU within the analysed timeframe while showing an inconsistent pattern in relation to the Cyber Diplomacy Toolbox. Overall, the UK has made seven statements. Three of these indicate autonomy, while three support common action. The UK also participated in drafting the 2018 non-paper. Looking back to 2017, it is evident that the UK's stance was

primarily focused on retaining autonomy regarding cyber diplomacy. The UK primarily expressed concerns that, as drafted at the time, the toolbox would constrain member states from pursuing unilateral action or collaborating with actors outside the EU: *"We would agree that these should largely fall to individual Member States, but where it is envisaged that the measures do not fall solely to a Member State, it is important to understand the circumstances. If authorization is deemed to be mixed or for the EU, would it limit an individual Member State's ability to act?"* (Council (3), 2017, p. 33). We repeatedly see these concerns in the UK's comments on the text. For example, the UK questioned a paragraph by saying: *"As drafted, this suggests that a Member State may not trigger a response without establishing a common position – is this a correct reading of this sentence?"* (Council (3), 2017, p. 33). While this paragraph does not explicitly call for autonomy, the questioning tone of the comment and the previous expression of autonomy suggest that this is also intended as a means of safeguarding the maneuverability of member states. The UK has also expressed support for retaining member state autonomy in matters of information sharing that could be used for attribution, stating that: *"Much evidence is likely to have come from classified channels and will be subject to disclosure restrictions -it is unlikely that any MS would want to or be able to share all supporting evidence with all MS. And in many cases Member States would not wish to publish any supporting evidence for a particular attribution. We would therefore recommend deleting this paragraph and replacing it with the wording from the G7 Declaration."* (Council (3), 2017, p. 35).

In 2018, we saw the UK take a stronger role regarding a common response and Europeanisation, calling for sanctions against Russian hackers (Guarisco, 2018, p. 2), as well as using the toolbox in response to potential election interference:*"*"*We should accelerate work on EU restrictive measures to respond to and deter cyberattacks, including a robust sanctions regime," urged British Prime Minister Theresa May in her summit statements "*(Brzozowski, 2018, p. 2).

As the UK left the EU beforehand, there are no comments on the EU's cyber posture. Overall, the statements suggest that the UK advocated retaining autonomy within the EU. However, the UK was not opposed to common action per se, but rather to excessive Europeanisation as perceived by the UK. While attempting to preserve the standing of member states and the option of unilateral action, the UK opposed the transfer of competence and Europeanisation.

Nevertheless, it supported the use of the toolbox and cooperation with EU member states outside of a formalised, EU-level agreement, thereby expressing support for the toolbox's ultimate goals. There are no statements from the UK indicating spillovers.

The UK is a particularly interesting case also from the perspective of uploading and cross-loading. In addition to the participation in the 2018 non-paper, the UK has made three statements that were coded as uploading and three coded as cross-loading. As previously discussed, attempts to upload by the UK were mostly focused on retaining the manoeuvrability of member states in relation to cyber diplomacy. The aim was to enshrine the established separation of powers and the sovereign right of member states to pursue whatever means they deem necessary, especially the sovereign right to attribute cyberattacks (see Council (3), 2017, pp. 33-35). Retention of manoeuvrability was apparently a national priority that was being uploaded. This is also evident when we look at the UK's efforts to retain autonomy over its information. As opposed to other states that were keen to establish information-sharing mechanisms, the UK tried to negatively upload its domestic priorities to the EU level by deleting paragraphs supporting obligatory information sharing. This would result in no mechanisms deemed constraining by the UK forcing member states to share information with others (Council (3), 2017, p. 35).

In terms of cross-loading there are three cases, the UK and the Netherlands provided cyber forensic information relating to cyberattacks in 2018 (Brzozowski, 2018, p. 1). This led to Council conclusions recognising the need to develop further measures regarding cyber diplomacy (Brzozowski, 2018, p. 1). This is in line with the UK's previous uploading priorities, as it is a willing supporter of the toolbox and common action, but is very keen to retain control over its information. However, it is not fundamentally opposed to sharing it, especially when it can lead to other member states supporting the UKs policy priorities. In other cases, the UK has acted within cross-loading coalitions, supporting EU sanctions against Russia in response to cyberattacks against the OPCW (Gessant, 2018, p. 1). The UK seemingly is willing to support such coalitions when they pursue their domestic goal of robust implementation of the toolbox, but not when it is 'forced' to do so or this would constrain them.

Comparison of findings

While it is not possible to reliably categorise all member states based on their behaviour, as their positions may change from statement to statement, some observations can be made about those that stand out the most.

Uploading was prevalent, with most member states expressing their preferences at the EU level in some way. France, Germany, the Netherlands, Denmark, the Czech Republic, Slovakia, Estonia, Latvia, Lithuania, the UK, Hungary, Finland and Sweden stand out as significant uploaders. Conversely, Romania, Austria, Malta, Greece and Bulgaria contributed to the toolbox but pursued uploading less actively than the other member states. Neither Luxembourg nor Croatia made statements in the examined corpus.

There is significant disagreement among some member states regarding NATO inclusion. Ireland's stance on NATO inclusion and cooperation mechanisms differs greatly from that of Lithuania and Latvia, who called for increased engagement. However, Ireland's position also differs from that of other neutral states at the time, such as Austria, Finland and Sweden. None of these states took issue with NATO inclusion or at least did not object to it in the examined corpus. In fact, Finland and Sweden welcomed NATO inclusion to some extent in their statements.

Regarding the role of presidencies, many member states have held the Council presidency within the examined timeframe. Some of which have taken steps to promote the toolbox. The presidencies examined that seem to have been the most prominent are those of France and the Netherlands. Nevertheless, other member states that were less active in other toolbox documents, such as Belgium, Romania and Malta, also promoted the toolbox when it was their turn to hold the presidency. Hungary, which can be regarded as a mixed candidate between Europeanisation and autonomy, also expressed support for work on cyber diplomacy during its presidency.

Cross-loading was more prevalent in some member states than in others, but no clear pattern emerged. From the direct statements observed, it appears that smaller member states are more likely to react to proposals made by other states, such as the Netherlands, the Czech Republic, Slovakia and Portugal. Except for Poland, larger member states did not refer directly to the

positions of other states, but were referenced more extensively by others, as was the case with Germany, which may indicate the role as a cross-loading leader. Many member states, especially larger ones, only engaged in cross-loading when involved in coalitions, such as with the non-papers. Hungary and Italy, which are more autonomy-oriented, did not participate in any non-papers or cross-loading coalitions. Ireland did not participate in the non-papers or engage in cross-loading, while the UK participated in cross-loading more extensively, also outside of non-papers.

Germany and France positioned themselves as cautious Europeanisers. Compared to some other states, they initially showed some reluctance and reservations regarding the development of the toolbox. While they endorsed the general goals, they did so with significant reservations; France was less reluctant than Germany. However, Germany then broadly endorsed and applied the measures. This can mostly be compared to Hungary's behaviour, where there was also some initial reluctance, but this was based on the desire to protect the sovereignty of member states. This differs from the German narrative, which simply cites uncertainty at that point.

Two patterns have emerged with regard to autonomy: on the one hand, there is 'genuine' autonomy, based on the will to respect the rights and privileges of member states from incursion by the EU, and on the other hand, there is a pattern of 'pragmatic' autonomy. Here, generally strong advocates of the toolbox, such as the Netherlands and the Baltic states and Sweden uncharacteristically drop out of their roles in order to favour not codifying or softening commitments in the proposed texts. This is presumably intended to achieve broad agreement among all member states, including those who advocate genuine autonomy. As we have seen, Sweden in particular introduced autonomy-supporting statements and then supplemented them with way-forward clauses. This was particularly evident in cases that touched on the previously identified core issues of information sharing and common attribution mechanisms. It seems as if the Europeanisers have realised that these issues are not easily solved. While countries such as the Czech Republic and Sweden are committed to developing mechanisms for these purposes, we have seen these issues sometimes being postponed or softened in the actual working documents, presumably in order to reach a consensus on the document.

Notably, other member states that occasionally present themselves as autonomists, such as the UK and Hungary, generally agree with the goals of the toolbox and express support for the

broader goals of the cyber diplomacy regime. However, they emphasise the need to respect their privileges when achieving these goals. When we compare the level of engagement of the UK and Hungary at the EU level with that of Italy, the poster child for autonomy, we see that Italy has garnered far more media attention due to its opposition. Italy has also manifested autonomy at the EU level, meaning that there is no clear connection between Europeanisation and uploading, or how member states behave when at the EU level. Personally, I would have expected the autonomist states to be more visible outside the EU negotiations and to 'retreat' from formal negotiations in the EU. Instead, autonomist states had to actively deviate more from the established consensus to express their preferences and were therefore probably more active overall. In contrast, some Europeanist states were able to take the back seat as others took the lead in Europeanisation of the toolbox.

A third group of member states could be considered tacit acceptors as they tend to agree with the established consensus and proposed texts, rarely expressing their views on the toolbox outside an EU context. Some occasionally amend the proposed text, Austria and Malta, for example, while others abstain almost completely, such as Bulgaria and Greece. Most tacit acceptors favour Europeanisation and often reiterate the Europeanist standpoint. This distinguishes them from the more active autonomist states, which deviate from the agreed text, and the active Europeanists, who are always engaged in furthering commitments and renegotiating.

From the above comparisons, we can draw conclusions in response to the literature gap identified by Tonra (2015, p. 192) regarding how member states diverge on policy consensus. Overall, the consensus emerging from the corpus is that the right of member states to attribute cyberattacks individually and to choose what information they share remains intact. Even if consultations were held, no formally binding mechanisms to this end were passed. Europeanisers such as Sweden and the Netherlands have amended the text to reflect this, demonstrating their adherence to the established consensus in formal negotiations. In contrast, some sovereignty-oriented states, such as Hungary and the UK, have pushed back against attempts to cross these red lines, while at the same time, subscribing to the general goals of the toolbox, which seem largely undisputed, even by the outlier Italy. At the same time, member states are committed to complying with international legal provisions and further developing the toolbox to ensure an effective cyber sanctions regime and avoid the issues. The adherence

to international law provisions were softened on occasion, but never outright rejected, this seems to be established consensus. At the same time, the consensus to include some mention of NATO was seemingly contested only by one neutral member state: Ireland. Member states diverge from the established consensus when the difference between the proposed text and their national priorities becomes too great. This often leads them to advocate for their priorities in the hope of creating a new consensus that takes these into account. In other cases, the established consensus is formed outside the formal EU arena, in cross-loading coalitions and related non-papers. Here, mutual information exchange first shapes policy, which is then brought to the EU table for discussion. We have seen no member state involved in such a cross-loading coalition diverge from the agreed non-paper position during negotiations after submission. Instead, instances where national priorities and consensus diverge slightly could be cases of tacit acceptance, with no changes being introduced to the document.

Postfunctionalism

Postfunctionalism provides a good interpretation of what we observed in the Italian case. The rejection of the toolbox is repeatedly said to be based on the preservation of Italian domestic economic interests. Here, it is argued that the greater economic threat actually stems from the EU enforcing the toolbox rather than from the economic threat posed by cyberattacks. In this case, therefore, we cannot speak of economic irrationality; rather, the economic agenda is being aligned with nationalist rhetoric and supported by nationalist forces from below the national level represented by businesspeople (see Euractiv.com with AFP, 2018, p. 1). In the case of Italy, I would argue that nationalist rhetoric is being presented as an economic argument in order to garner support based on the prevalence of economic arguments brought forward and the interest of the businesspeople. At the same time, the close relationship reported between the Italian and Russian governments may also have contributed to their opposition to the toolbox. Personally, I would have expected Hungary to behave similarly regarding sanctions against Russian actors, but this is not evident in the toolbox. At no point in the corpus does Hungary base its argument on anything other than the text's ambiguity or the retention of the existing member state monopoly on attribution and information sharing. In contrast to Italy, Hungary never refers directly to Russia or shows evidence of pushback by nationalist forces.

Conversely, the expectation of Europeanisation in post-functionalist theory is generally realised in most other member states examples, as no other member states invoke national

interest groups to justify opposition to the toolbox. The 'economically rational' narrative prevailed where defence of the toolbox was perceivedas more important by the elites negotiating at EU level because it seemed to defend economic motives. Meanwhile, it was hardly salient at national level, perhaps even being perceived as a technocratic EU issue. This explains why the calling on nationalist forces below state level was not a recurring pattern. When we have seen sub-state actors acknowledge the toolbox, for example, when the Dutch VVD called for its application in parliament (see Leeson, 2022, p. 1), we have not seen a nationalist backlash. Rather, we have seen an expansion of the perceived national threat posed by cyberattacks against the Netherlands to the European level. The lack of nationalist pushback in this case may be because there is no loss of member state sovereignty here but an attempted uploading of the national threat to the European level.

Regarding tacit acceptance, postfunctionalists might view this scenario as an instance in which Europeanisation can progress largely unhindered at the European level due to a lack of politisation at lower levels of the toolbox. Statements created by the EEAS or the respective presidency satisfy member states and the elites representing them who do not wish to interfere with the current path of Europeanisation fuelled by economic interests.

Intergovernmentalism

The core tenets of intergovernmentalism were evident in our case, with member states presenting themselves as the central actors engaged in economy-oriented bargaining. However, defence and security-based argumentations, as well as human-rights based argumentations were also important factors that appeared to be the basis for development of the toolbox. States were reluctant to give up some of their core competencies. Although some member states advocated for this, states could not be made to accept things that went against their interests. Due to the scope of the thesis, the EU Commission and Parliament played a very small role in the examined corpus; states remained the main actors throughout the development.

The three-step process of intergovernmentalism was evident in our case: *'the domestic formation of national preferences; intergovernmental bargaining; and the creation of European institutions to secure agreements'* (Hooghe & Marks, 2019, p. 1116), but the main issue was that the creation of institutions, or rather the expansion of their competencies, was also one of the core subjects of intergovernmental bargaining and repeatedly hindered by some

member states, but ultimately adopted nonetheless. The majority of statements were after all clearly in favour of Europeanisation where member states are in favour of the creation of new mechanisms.

The issue of asymmetrical interdependence between member states was complicated in the context of negotiations for the Cyber Diplomacy Toolbox. The members affected by cyber threats were the most likely to argue for its application, except in the case of Ireland. However, regarding the development of the toolbox at least, the perceived threat to member states does not sufficiently explain their behaviour. For example, Poland, which was the victim of a cyberattack during the period under review, could have been expected to play a more proactive role in the development of the toolbox, at least after the attack, which was not the case. However, the assumption that member states with important relationships with the sanctioned states would be unwilling to harm their economic relationship proved to be true at least in the case of Italy and Russia .Given the significant trade relationships that many EU countries have with China, this may also help to explain why China was only mentioned once in the corpus.

The intergovernmentalist idea that Europeanisation maintains commitments between governments cannot be proven or disproven in the case of the toolbox. As we have seen, Italy rejected the idea of establishing a coordination group, probably to ensure the capacity to deviate from the common track in future. The development of the toolbox still prioritised unanimity, and member states, including pro-European governments, did not systematically argue for binding themselves to common decision procedures, however the willingness increased over time. Even in the case of generally pro-Europeanisation states such as Latvia, it has been argued that attribution will always be on a case-by-case basis. Thus, it has been suggested that member states should be allowed to withdraw from the application of the toolbox. Even if coordination was favoured, member state primacy seemed to prevail overall. This aligns with the notion that lowest-common-denominator politics prevail.

Intergovernmentalism also provides possible explanations for the pattern of tacit acceptance. It offers two interpretations of this phenomenon. Firstly, in cases of tacit acceptance, the text may already represent the lowest common denominator and is therefore widely accepted. Secondly, the toolbox development follows an economically rational logic in an attempt to avoid large discrepancies. In cases such as the Latvian example (see Council (3), 2017, p. 18),

states at economic risk actively shape the toolbox, while states whose economies are less at risk choose not to interfere or set the pace.

Neofunctionalism

As we have seen, spillover tendencies occurred on multiple occasions. Overall, it seems that most member states agreed that the development of the toolbox was the goal. Effective Europeanisation presented itself as a solution to the issue of cyber threats which led to a shifting of expectations to the EU level. Recalling the German, Estonian, Polish and Dutch cases, national actors deliberately shifted their expectations regarding defence against cyberattacks to the EU level to achieve protection.

Not only was there functional spillover based on economic rationale, but previous commitments in defence and cybersecurity also exerted pressure to develop the toolbox. Considering the development of the toolbox in response to cyberattacks, it is evident that exogenous stimuli and perceived threats played a role in prompting member states to endorse a Europeanised toolbox and coordinated action. However, examining the exogenous factors that could influence Europeanisation, the impact of the war against Ukraine, could not be verified in the analysis of the toolbox's development. Even if Ukraine is not a member state, the war could still work as an exogenous stimulus, this contrasts with the idea of crisis-driven integration. We have, however, seen some integrative efforts in response to individual cyber-attacks against member states, as was the case following the attacks on the OPCW, the Netherlands, Estonia and Germany.

If we also look at the influence certain member states have held due to the informational advantages, such as the Netherlands and the UK, but also Estonia and Germany when calling for application of the toolbox, this relates to the claims in the literature that member states that are actively involved, such as those previously mentioned, are more likely to succeed in achieving a common response (see Sachs et al., 2024, p. 18)

Due to the scope of this thesis, there were few instances of cultivated spillover, as the focus was primarily on the efforts of the member states. Nevertheless, we found that the EEAS was a significant contributor, having been granted the authority by the member states on occasion to suggest and develop proposals for the toolbox, although the member states always retained the right to approve or reject suggestions. Lastly, considering path dependence, we can see

some indicators of path dependence especially in the cautious Europeanisation and tacit acceptance pattern, for example in the statements of some member states and the references to previous commitments in the field of cyber diplomacy and other fields. However, the pressure from spillover is still too weak to breach the 'hard barriers' of attribution and information sharing, perhaps due to a lack of societal, external and ideational preconditions of integration (see Rosamond, 2005, p. 249) that neofunctionalism bases itself on. Path dependence is evident in the non-papers, for example, where the history of the toolbox and previous EU commitments are invoked, and in the Latvian attempt in 2017 to include NIS bodies in the Cyber Diplomacy Toolbox infrastructure, which illustrates a continuity in Europeanisation efforts and the potential expansion of an EU body's powers. Conversely, there has also been pushback against such efforts to expand the competencies of certain NIS bodies, as demonstrated by the Netherlands, for example.

Europeanisation of Foreign Policy

Member states engaged in significant uploading based on their national preferences but also applied the 'handbrake' when their domestic objectives seemed threatened, as was the case for the UK, Ireland and Italy. Overall, the larger member states were more reluctant to approve Europeanisation with regard to the toolbox but seemed to become more accepting of it over time. Contrary to Wong and Hill's assumption that smaller member states would play a less active role in developing the toolbox (see Wong & Hill, 2011, p. 10), a select few smaller member states played more important roles than would have been initially thought, at the same time it proved true that other member states such as Greece, Romania and Bulgaria, while promoters of the toolbox, seemed to be dragged along. Germany, France, Italy and the UK took prominent roles in shaping the toolbox while conversely, other larger states, such as Poland and Spain, were expected to play a more significant role. Similarly, smaller member states such as Estonia, the Netherlands, Denmark and the Czech Republic played disproportionately large roles. Wong and Hill led us to expect this, as some member states are being pushed into new fields in which they have expertise. At the same time, they must adhere to agreed European positions in order to fulfil their national priorities and present them as European priorities (see Wong & Hill, 2011, p. 7). While it cannot be determined which states adapted to common EU positions the most, the larger member states could deviate from the common position more

significantly and prioritise autonomy-oriented positions, as evidenced by early French, Italian and UK statements.

Overall, it is clear that some form of Europeanisation has taken place, as member states have consistently responded to changes at the EU level and, in some instances, appeared to converge on shared positions (Tonra, 2015, p. 190). At the same time, it appeared that the common European standpoint was influenced by the preferences of member states, while also often resisting the preference of a single member state. For example, France's initial reluctance to use the word 'deterrence' and Ireland's opposition to including NATO in the toolbox text were not reiterated by the member states in the following texts. Another recurring theme was that creating a common position appeared to be a policy preference for many member states, potentially causing them to compromise on other priorities. This is evident from the statements of the Dutch, Lithuanian and Latvian governments. Examining the substantial cross-loading in the Czech Republic, it is evident that changes to the toolbox were derived from proposals and information exchanged with other member states to establish a unified European stance. Member states presumably introduced autonomist statements to make the text acceptable to all. This also sheds light on the tacit acceptance response pattern, whereby member states preferred not to introduce their domestic policy changes corresponding to their perfect priorities, rather than risking the complete discussion and reworking of the established text which seemed acceptable to most.

Considering the research questions

How have EU member states influenced the development of the EU Cyber Diplomacy Toolbox?

The development of the toolbox appears to have been driven primarily by member state advocacy and utilisation. Except for Luxembourg and Croatia, all EU member states have taken measures to influence the toolbox throughout its development. Overall, the corpus includes a wide range of statement numbers from each member state. Contrary to what Wong and Hill (2011, p. 10) might suggest, the number of statements from each member state does not reflect its relative size in CFSP matters. At the same time, there was a tug of war between member states that generally supported the toolbox goals but were unwilling to give up their powers and those that saw the toolbox as ineffective if a common mechanism under EEAS leadership was not possible. This conflict in the further development of the toolbox while still not touching

on core member state privileges seems to be the common thread that ties the development of the entire toolbox together.

Some member states have paid particular attention to including their preferences in the toolbox texts. Ultimately, however, member states have played a two-faced role in the development of the toolbox. While many member states have expressed support, in some cases they have also expressed and shaped the toolbox to respect their privileges and sovereignty rights in CFSP matters. Overall, member states have paid cautious attention to this, and support by member states can be described as conditional, whether their preferences are considered. Whether the toolbox would have been more or less ambitious had member states had less say in its development is hard to say. Personally, I suspect that without advocacy from the member states, the toolbox would have been less ambitious in pursuing its cyber diplomacy goals and would have implemented weaker measures. In any case, if the member states had not used the toolbox measures in response to attacks, the subsequent calls for development of the toolbox, such as after the OPCW attack (see Gessant, 2018, p. 1) would not have occurred.

Although member state advocacy for the toolbox was the driving factor, it was also necessary to consider the views of the other member states and reach compromises. Conversely, constant pushback and reluctance to exceed what had been agreed hindered the development of a more ambitious toolbox. Member state preferences vary, but can mainly be classified according to geographical, economic and defence topics. Geographical topics include a focus on certain geographical areas and states, while economic topics include protecting domestic businesses or maintaining good trade relations with certain states. Defence narratives emphasise the importance of deterrence, and cybersecurity topics tie into all of these. Preferences are also expressed in terms of what the toolbox should look like. Member states repeatedly try to link the toolbox and its measures to existing initiatives and EU infrastructures. Conversely, member states are pushing back against what they perceive to be an unjustified expansion of competencies. They also have different views on information sharing and common attribution. These differences have repeatedly resulted in changes to the toolbox and its contents to align with the preferences of the member states. There was a recurring need to formulate the texts in such a way as to ensure that the toolbox is functional and usable while not restricting the individual action of member states or forcing them to pursue actions that are against their interests.

Do governments attempt to upload or cross-load national preferences in their statements?

Most states have published their national priorities in statements and attempted to implement them at the European level. Some member states are more vocal than others when it comes to uploading their preferences; the most notable of these include France and the Netherlands. The pattern of tacit acceptance plays a role here: we have seen some member states choose not to introduce changes to large parts of certain texts but still resubmitted the texts as part of document drafts, thereby implying support. Strict uploading attempts to the EU level according to concrete national policy examples remains rather rare; uploading attempts mainly take the form of preference formulation at the EU level based on national policy preferences. This form of uploading attempt is prevalent in the corpus, both in support of Europeanisation but also in the retention of autonomy. Compared to uploading, cross-loading remains a rarer phenomenon. Member states have formed coalitions to promote the toolbox and engage in policy information exchange. While some member states are particularly active in cross-loading formulations, reacting continuously to statements by others, others choose to 'do their own thing', disregarding the position of other member states in their concrete policy proposals and aligning themselves with others only in pursuit of broader goals. Estonia, Czechia, and the Netherlands stand out as substantial cross-loaders, whereas Germany stands out as a cross-loading leader. Unlike uploading, cross-loading arguments noticeably favoured Europeanisation, with autonomy playing almost no role.

Which governments support or oppose transferring competences to the EU, and do their documented positions reveal spillover tendencies?

We have a clear overrepresentation of support for the toolbox and its measures. Most member states agree on the need for a common response, with Italy being the most notable exception, as it has put forward the most detailed case against the toolbox and in favour of autonomy. Generally based on the corpus most other member states should be classified as proponents of the toolbox. It is unclear whether it is warranted to classify Hungary and the UK as opponents of Europeanisation of the toolbox. Their statements do include a significant amount of sovereignty codes, but in general, it emerges that they are not opposed to the concept of the toolbox itself but rather the competency transfer to the EU level.

However, while member states generally support the toolbox and its measures, there is often some opposition when the specific measures are examined in more detail. For instance, regarding a mechanism for the EU CSIRT network to contact the CSIRTs of non-EU member states, even the proponents, France and the Netherlands, were reluctant to entrust this task to the EU's CSIRT network. At the same time, Latvia was clearly in favour of this. Ultimately, while there is pushback against Europeanisation, this mainly stems from a few states against a backdrop of rather ambitious working documents and proposals. While some member states explicitly oppose these text paragraphs, most choose not to interfere and allow Europeanisation to continue.

Surprisingly, some member states that are generally in favour of Europeanisation also make statements referencing autonomy, such as the Netherlands, Sweden and France. As we have seen, this is mainly the case when an issue touches on a member state's core privilege, such as the right to retain control over information or to respond to and attribute cyberattacks individually with non-EU partners. As mentioned at the beginning of the thesis, information sharing and attribution remained the biggest obstacles to creating a Europeanised toolbox. In a few cases, member states have supported setting aside such privileges to ensure an effective toolbox. Nevertheless, paragraph 26 of the draft Council conclusions on the EU's cybersecurity strategy for the digital decade shows that no member state has chosen to alter or delete the reference to*: 'in full respect of national competences and prerogatives'* (Council, 2021, p. 16). This demonstrates that even member states that generally support Europeanisation are reluctant to infringe on established competencies to their own detriment. Although we have seen the EEAS support the idea of introducing QMV in toolbox matters (European Commission, 2020, p. 17), none of the over 200 statements by member states expressed this opinion. Even the most pro-European member states did not introduce the idea of giving up veto rights or introducing QMV in relation to the toolbox. An emerging pattern throughout the development of the toolbox is that of cautious Europeanisation, wherein member states are at first cautious to commit to any degree of Europeanisation, such as in the German case, and then become more willing over time to commit to a degree of Europeanisation over time in their proposals to pool information and create a common mechanism.

Spillover plays only a minor role in the arguments of most member states. It is mainly evident in the case of the NIS Directive or when considering overarching security or economic goals.

Spillover arguments are primarily presented as part of non-papers to pursue a common response, rather than to validate specific changes to working texts. Issues most often raised outside of the specific cybersecurity goal that distinguishes the field of cyber diplomacy are general physical and hybrid security and, most frequently, critical infrastructure and general trade and economic concerns. However, as we have seen, economic considerations can facilitate spillover, with the development of a toolbox being put forward as a means to deter economic damage. Conversely, as in the Italian case, economic considerations can be used to legitimise opposition to Europeanisation by citing the importance of international trade and relations with the sanctioned country.

Link to the literature

The findings are directly related to the literature on the toolbox, which has already identified information sharing and common attribution as the main obstacles to an effective and unified Cyber Diplomacy Toolbox (see Moret et al., 2017, pp. 3-4). Member states also pursue joint action with external actors when they deem EU joint action to be inadequate; for example, the UK and the Netherlands have done so in the past with the U.S. (see Brzozowksi, 2018, p. 2). In addition, we have found that when actors deem national action alone to be insufficient, they also seek a common European response. Examples of this include the German, Dutch, Polish and Estonian cases.

Ivan (2019, pp. 5-7) identified the Netherlands, Denmark and the UK as attributors of cyberattacks, whereas Italy was depicted as being more reluctant to do so. Our findings generally support this, but Poland, Germany and Estonia may also be considered as potential attributors, given that these member states have actively used the toolbox. In contrast, Ireland appeared reluctant to use the toolbox when attacked. Belgium, Sweden and Finland have emphasised the importance of using less escalatory measures before resorting to the cyber sanctions regime.

Regarding the role of NATO and the EU, we have observed a shift. Previously, the EU focused on cybercrime, whereas state-sponsored malicious cyber activities were regarded as NATO's domain (Štitilis et al., pp. 1156–1157). However, the EU has started to encroach more and more into NATO's domain in this regard, focusing more on state-sponsored activities, as evidenced by the development of the toolbox. Member states have different relationships with NATO and

seek various levels of NATO inclusion in the toolbox. It cannot simply be said that neutral countries oppose NATO inclusion and that NATO members support it. Proponents especially value information-sharing agreements, and cooperation with NATO generally poses no problem for most member states. Nevertheless, there has been some opposition to an overly militarised relationship in cyber diplomacy with non-EU countries.

Regarding the effectiveness of the toolbox as a deterrent. As discussed in the literature, definitive statements cannot be made. Nevertheless, it is evident that the deterrent effect of the toolbox is very present in the member state perception of it, the deterrent effect is often cited as a justification for its existence and the ongoing development of the Cyber Diplomacy Toolbox. Although we have seen member states use toolbox measures in response to cyberattacks, this has generally happened years after the attacks occurred. Therefore, its real-world effectiveness cannot be confirmed or denied. However, the deterrent effect of the toolbox is at least recognised by member states as a recurring theme.

In literature on the application of the toolbox, the war in Ukraine has been cited as a major catalyst (see Sachs et al., 2024, p. 10) for many applications. We cannot observe a spike in development following the outbreak. Its impact seems limited in the corpus we observed. There were no concrete references to the war in the corpus, which contrasts with the toolbox application as described by Sachs and colleagues (2024, p. 10).

Conversely, we found that the EU's reputation as a standard setter and promoter of best practices and adherence to international law is well-founded (see Latici, 2020), as these qualities were evident in many of the statements examined. Member states generally seem to subscribe to these goals and actively promote them within the EU, particularly with regard to adherence to international law and human rights, as well as technical standards such as data protection. Member states appear to view the toolbox as a means of propagating their standards beyond the EU. In multiple statements, we found references to establishing a common EU position at the UN, for example, regarding cyber standards as part of cyber diplomacy.

6. Conclusion

What have we found

If we consider the question; "*How have EU member states influenced the development of the EU Cyber Diplomacy Toolbox?"*, we can see that while promoting the toolbox, it could be argued that member states have also set out clear boundaries that their competencies must be respected with regard to the distribution of powers between the EU and its member states. Member states have voiced their varied priorities at the EU level, either to further develop the toolbox or to remove certain elements from it and even retain their autonomy. Most member states have come to accept the toolbox as a legitimate means of strengthening their cyber diplomacy and deterrence and as such some use its measures more frequently than others. Overall, it can be concluded that Europeanisation in the field of cyber diplomacy, specifically with regard to the Cyber Diplomacy Toolbox, is progressing slowly. Some member states are setting the pace for this progression but there is limited pushback against it, which remains confined to a select few core member state privileges.

Member states actively pursue their interests at the European level to fulfill their national preferences. However, they also deviate from common positions when these contrast sharply with their perceived domestic interests. Member state positions have remained relatively stable over time. Some member states 'warmed up' to the toolbox as part of cautious Europeanisation, recognising its usefulness, as well as that of common action and Europeanisation. Interestingly, some pro-Europeanisation member states have expressed support for protecting member state privileges in the CFSP, as well as pushing back against certain EU bodies' spillover and enlargement of powers. 'Tacit acceptance' describes statements made in the context of the toolbox that did not introduce substantial changes. This suggests that many member states generally deem common measures to be acceptable. Cross-loading is common in coalition contexts where multiple member states seek to shift the EU's position. However, it can be said that smaller member states are more likely to react to cross-loading and acknowledge proposals from other member states outside of cross-loading coalitions, as opposed to larger member states for which this was comparatively less observed. Most member states engage in uploading to some extent in line with their preferences. Uploading is not limited to Europeanisation cases but can also be observed in cases where respect for sovereignty and member state rights is advocated. In contrast there are no cases of autonomy being cross-loaded. Spillover is also

relevant in cross-cutting issues, touching on the economy, defence, human rights, and hybrid warfare and disinformation. These issues exert spillover pressure to deepen collaboration on the toolbox. Overall, spillover is most prominent in non-papers compared to news articles or working documents and the NIS institutions and mechanisms are particularly often invoked as forums where the toolbox can be linked to other fields and existing infrastructures. Information sharing and mutual attribution remain key issues, though no member state has directly called for the abolition of unanimity and the introduction of qualified majority voting in matters relating to the toolbox.

Theoretical and practical takeaways

Based on the three theories, some of what we have seen can be explained. The arguments in favour of intergovernmentalism were straightforward. Member states clearly formulate preferences and engage in bargaining, partially exemplified by cross-loading, which can lead to institutional expansion at the EU level. While member states have voiced their preferences at the EU level, the expansion of competencies has been the most crucial issue debated by member states. In a scenario where the need for common action seems to be agreed by most states, the shape or form that institutional expansion takes is of core importance.

Regarding neofunctionalism, we have seen that, to a certain extent, member states have turned to the EU for help in meeting their cybersecurity needs, particularly through cyber diplomacy and the toolbox. Conversely, we have observed spillover tendencies from other fields influencing the development of the toolbox. Previous commitments have also played an important role in exerting path dependence towards further Europeanisation.

Through the lens of postfunctionalism. We have seen that credible opposition to the toolbox and its measures can be constructed based on nationalist forces below the state level, as demonstrated by Italy in particular. At the same time, we must acknowledge that an economic rationale has been employed to justify this as well. For the majority of member state cases, no nationalist pushback was observed, potentially due to the lack of politicisation of the toolbox as a topic in the national sphere.

In terms of the Europeanisation literature of Hooghe and Marks, we have seen that the special relationship with non-EU states has affected member state preferences and, in turn, the development of the toolbox, sometimes hindering it. Conversely, many of the statements

observed prioritise formulating a common European response. The formulation of a common European framework is something that almost all member states can agree on as long as it does not infringe or constrain their rights. This may explain why some of the most fervent proponents of European integration have sometimes favoured member state sovereignty as their desire to establish a common European standpoint may have outweighed the need to create a robust toolbox. This phenomenon is worth further investigation, particularly in cases where Europeanisation in the form of finding a common standpoint involves accepting less constraining and ambitious texts.

Personally, I believe there are three general takeaways for member state behaviour in CFSP. Firstly, member states generally subscribe to common goals and objectives, but how these are achieved is equally, if not more, important in ensuring support from all parties. Secondly, member states are especially reluctant to bind themselves when they feel that their national priorities are at risk. Member states are unlikely to breach certain red lines regarding issues of attribution and information sharing *and* are likely to look for workarounds rather than address these issues directly. Lastly, when they feel that unilateral action on their part will not solve the problem, member states actively try to present their national priorities as common European priorities and their nationally perceived threats as common European threats.

In conclusion, it can be said that member states have had a significant impact on the development of the toolbox. Especially based on the expressions of their domestic preferences, and their behaviour at EU-level.. The perpetual tug of war between Europeanisation and sovereignty has been the leitmotif of its development, but the toolbox's ultimate effectiveness as a deterrent will depend on whether member states can eventually overcome these differences.

Future research and limitations

As much of the corpus consists of statements made at the EU level, such as in working groups, it is unsurprising that most statements coded support Europeanisation, especially given the broad definition employed. The research was limited by the fact that many potentially relevant documents were not publicly available at the time, so I had to work with what was accessible. The Cyber Diplomacy Toolbox appeared on the agenda of the Council's Horizontal Working Party on Cybersecurity 20 times in 2024 alone. Despite my efforts, these documents are mostly

classified and inaccessible to the public, so they do not form part of the corpus. Many of these agenda items address input from the EEAS concerning the transmission of situational awareness, as well as the sharing of information and explanations of EU efforts with delegations. Future research may attempt to access these files. Sachs, Schmalfeldt and Zettl-Schabath (2024, p. 21) also recognise the importance of Russia's war against Ukraine in the application of the Cyber Diplomacy Toolbox. However, in the evaluated corpus, this has played a very limited role, suggesting a potential blind spot that could be addressed by examining statements made by the EU, rather than the member states on the development. It would also be beneficial to shift the focus from the member states to the roles of the EEAS and the Commission in cultivating spillover and pushing for more development. Conversely, one might also examine the role of the toolbox in the cybersecurity and cyber diplomacy strategies of individual member states at a domestic level. During my research, I came across some references to it, but not from all member states. Finally, it would be interesting to examine how presidencies promote CFSP policy in relation to Europeanisation. As we have seen, presidencies played an important role in promoting the toolbox. Future research could examine the behaviour of member states before, during, and after a Council presidency to see how it relates to their stance on the toolbox.

Personally, I would have liked to see more statements from almost all member states, particularly from Luxembourg and Croatia, in order to be able to comment on the views of all member states. I was tempted to expand the scope of material I collected beyond the identified sources, but in the end, it seemed as if this would make it difficult to clearly identify where to start and stop the search. Perhaps the thesis could have benefited from a more focused theoretical perspective; by giving all three theoretical strands equal attention, I aimed to avoid personal bias and offer a broader perspective on the explanatory patterns behind the development of the toolbox.

7. Sources

Aggestam, L./Bicchi, F. (2019): New Directions in EU Foreign Policy Governance: Cross-loading, Leadership and Informal Groupings. In: JCMS: Journal of Common Market Studies, 57(3), p. 515-532. Oxford: Blackwell Publishing Ltd. Retrieved from: https://doi.org/10.1111/jcms.12846.

Alatalu, S./Austin, G. (2020): Alliance attribution of global cyber attacks: The European Union. In: Austin, G. (Eds.): National Cyber Emergencies, p. 171-185. United Kingdom: Routledge. Retrieved from: https://doi.org/10.4324/9780429343438-10.

Attafa, A./Renaud, K./De Paoli, S. (2020): Cyberdiplomacy: A systematic literature review. In: Procedia Computer Science, 176, p. 60-69. Elsevier B.V. Retrieved from: https://doi.org/10.1016/j.procs.2020.08.007.

Auswärtiges Amt (2020): Non-Paper on EU Cyber Diplomacy by Estonia, France, Germany, Poland, Portugal and Slovenia. Berlin. Retrieved from: https://www.auswaertiges-amt.de/resource/blob/2418986/206b3bf9aa4ef45a2887399231840d23/201119-non-paper-pdf-data.pdf [last accessed on 28.04.2025].

Belgian Council Presidency (2024): PROGRAMME Belgian Presidency of the Council of the European Union First half of 2024. Retrieved from: https://wayback.archive-it.org/12710/20241018101819/https://belgian-presidency.consilium.europa.eu/en/ [last accessed on 24.09.2025]

Bendiek, A. (2018): The EU as a force for peace in international cyber diplomacy. Berlin, Stiftung Wissenschaft und Politik SWP, Deutsches Institut für Internationale Politik und Sicherheit. Retrieved from: https://nbnresolving.org/urn:nbn:de:0168-ssoar-57428-2 [last accessed on 14.07.2025]

Benoit, K. (2020): Text as data: an overview. In: L. Curini./R. Franzese (Eds.): Text as data: an overview. Vol. 2, London, SAGE Publications Ltd., p. 461-497 Retrieved from: https://doi.org/10.4135/9781526486387.n29

Bertuzzi, L. (2023): EU countries mull strengthening cooperation on digital diplomacy. Euractiv. Retrieved from: https://www.euractiv.com/news/eu-countries-mull-strengthening-cooperation-on-digital-diplomacy/ [last accessed on 16.09.2025].

Bertuzzi, L. (2024): Belgian presidency pitches EU Council overhaul over digital diplomacy. Euractiv. Retrieved from: https://www.euractiv.com/section/tech/news/belgian-presidency-pitches-eu-council-overhaul-over-digital-diplomacy/ [last accessed on 16.09.2025].

Brzozowski, A. (2018): Fearing election hacking, EU leaders to ready sanctions. Euractiv.com with Reuters. Retrieved from: https://www.euractiv.com/section/tech/news/fearing-election-hacking-eu-leaders-to-ready-sanctions/ [last accessed on 11.09.2025].

Bulmer, S./Lequesne, C. (2020): 1. The European Union and its Member States: An Overview In: Bulmer, S./Lequesne, C (Eds.):The member states of the European Union. (3rd edn). Oxford: Oxford University Press. Retrieved from: https://doi.org/10.1093/hepl/9780198737391.001.0001

Carver, J. (2024): More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. In: Journal of European Public Policy, 31(8), p. 2250-2286. Retrieved from: https://doi.org/10.1080/13501763.2023.2295523.

Council (2017)(1) Council of the European Union : Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") 10474/17, 19 June 2017. Brussels. Retrieved from: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf [last accessed on 13.05.2025].

Council (2017)(2), Council of the European Union Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities 13007/17, 9 October 2017. Brussels. Retrieved from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [last accessed on 15.07.2025].

Council (2017)(3), Council of the European Union:Joint Diplomatic Response to Cyber Operations (Cyber Toolbox)- Member States' comments 8146/1/17, 8 May 2017. Brussels. Retrieved from: https://data.consilium.europa.eu/doc/document/ST-8146-2017-REV-1/en/pdf [last accessed on 10.09.2025].

Council (2017)(4), Council of the European Union : Draft Council Conclusions on a Joint Diplomatic Response to Cyber Operations (Cyber Toolbox) - Compilation of comments 8907/17 11 May 2017. Brussels. Retrieved from: https://data.consilium.europa.eu/doc/document/ST-8907-2017-INIT/en/pdf [last accessed on 10.09.2025]

Council (2019)(1), Council of the European Union): Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, L 129 I/1. Brussels. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0796 [last accessed on 17.04.2025].

Council (2019)(2), Council of the European Union : Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, L 129 I/13. Brussels. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019D0797 [last accessed on 17.04.2025].

Council (2021), Council of the European Union : WORKING PAPER Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade WK 1754/2021 INIT. Brussels. Retrieved from: https://data.consilium.europa.eu/doc/document/WK-1754-2021-INIT/en/pdf [last accessed on 09.09.2025].

Council (2022), Council of the European Union : Draft Council conclusions on the development of the European Union's cyber posture 8594/22. Brussels. Retrieved from: AGENCE EUROPE https://aeur.eu/f/1km [last accessed on 10.09.2025]

Council (2023)(1),Council of the European Union :Council Decision (CFSP) 2023/964 of 15 May 2023 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, L 129/16. Brussels. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023D0964 [last accessed on 16.05.2025].

Council (2023)(2), Council of the European Union : Revised Implementing Guidelines of the Cyber Diplomacy Toolbox. Council Document 10289/23, 8 June 2023. Brussels. Retrieved from: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf [last accessed on 13.05.2025].

Council (2025), Council of the European Union : Council Implementing Regulation (EU) 2025/173 of 27 January 2025 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. Brussels. Retrieved

from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32025R0173 [last accessed on 17.04.2025].

Danish Presidency Council of the European Union (2025): Programme of the Danish EU Presidency. Retrieved from: https://danish-presidency.consilium.europa.eu/en/programme-for-the-danish-eu-presidency/programme-of-the-danish-eu-presidency/ [last accessed on 09.09.2025].

DK/EE/FI/LT/LV/NL/RO/UK non-paper (2025): EU Cyber Restrictive Measures: DK/EE/FI/LT/LV/NL/RO/UK non-paper. Retrieved from: https://www.politico.eu/wp-content/uploads/2018/10/POLITICO-non-paper-cyber-sanctions-regime-OCT-10.pdf [last accessed on 19.09.2025].

Euractiv.com with AFP (2018): Salvini 'at home' in Moscow, denounces EU sanctions on Russia. Retrieved from: https://www.euractiv.com/section/global-europe/news/salvini-at-home-in-moscow-denounces-eu-sanctions-on-russia/ [last accessed on 26.09.2025].

Euractiv.com with AFP (2020)(1): Germany calls in Russian envoy, seeks sanctions over hacking. Retrieved from: https://www.euractiv.com/section/tech/news/germany-calls-in-russian-envoy-seeks-sanctions-over-hacking/ [last accessed on 26.09.2025].

Euractiv.com with AFP (2020)(2): EU, UK slap sanctions on Russian spies for hacking German parliament. Retrieved from: https://www.euractiv.com/section/global-europe/news/eu-uk-slap-sanctions-on-russian-spies-for-hacking-german-parliament/ [last accessed on 10.09.2025].

European Commission (2018): JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Increasing resilience and bolstering capabilities to address hybrid threats JOIN(2018) 16 final. Brussels. Retrieved from: https://www.eeas.europa.eu/sites/default/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf [last accessed on 08.07.2025].

European Commission (2020): JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital

Decade JOIN(2020) 18 final. Brussels. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018 [last accessed on 07.07.2025].

European Parliament (2018): Cyber defence. P8_TA(2018)0258 European Parliament resolution of 13 June 2018 on cyber defence (2018/2004(INI)). Brussels. Retrieved from: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0258_EN.html [last accessed on 03.05.2025].

European Union (2008): Consolidated version of the Treaty on European Union, TITLE V - GENERAL PROVISIONS ON THE UNION'S EXTERNAL ACTION AND SPECIFIC PROVISIONS ON THE COMMON FOREIGN AND SECURITY POLICY, Chapter 2: Specific provisions on the common foreign and security policy, Section 2: Provisions on the common security and defence policy, Article 42. Official Journal of the European Union, C 115/38-39. Brussels. Retrieved from: http://data.europa.eu/eli/treaty/teu_2008/art_42/oj [last accessed on 28.04.2025].

European Union (2016): Consolidated version of the Treaty on the Functioning of the European Union, PART FIVE - THE UNION'S EXTERNAL ACTION, TITLE VII - SOLIDARITY CLAUSE, Article 222. Official Journal of the European Union, C 202/148. Brussels. Retrieved from: http://data.europa.eu/eli/treaty/tfeu_2016/art_222/oj [last accessed on 28.04.2025].

French Council Presidency (2022): Draft Council conclusions on the development of the European Union's cyber posture. Brussels. Retrieved from: AGENCE EUROPE https://aeur.eu/f/1km [last accessed on 25.09.2025].

Gessant, C.C. (2018): European leaders expected to call for sanctions against perpetrators of cyber attacks. Bulletin Quotidien Europe 12119. Brussels. Retrieved from: https://agenceurope.eu/en/bulletin/article/12119/3 [last accessed on 09.09.2025].

Gessant, C.C. (2019): EU is making progress in developing a penalty regime applicable to perpetrators of cyber attacks. Bulletin Quotidien Europe 12192. Brussels. Retrieved from: https://agenceurope.eu/en/bulletin/article/12192/31 [last accessed on 09.09.2025].

Gessant, C.C. (2021): EU leaders condemn latest cyber attacks and call for response. Bulletin Quotidien Europe 12749. Brussels. Retrieved from: https://agenceurope.eu/en/bulletin/article/12749/15 [last accessed on 15.09.2025].

Gessant, C.C. (2025): EU sanctions three GRU officers found responsible for cyber attacks against Estonia. Bulletin Quotidien Europe 13566. Brussels. Retrieved from: https://agenceurope.eu/en/bulletin/article/13566/29 [last accessed on 15.09.2025].

Guarisco, F. (2018): Italy resisting EU push to impose sanctions over cyberattacks. Reuters. Retrieved from: https://www.reuters.com/article/technology/italy-resisting-eu-push-to-impose-sanctions-over-cyberattacks-idUSKCN1MM2CP/ [last accessed on 11.09.2025]

Hartmann, T. (2023): Technological independence key focus in Germany's China strategy. Euractiv. Retrieved from: https://www.euractiv.com/section/tech/news/technological-independence-key-focus-in-germanys-china-strategy/ [last accessed on 15.09.2025].

Hooghe, L./Marks, G. (2019): Grand theories of European integration in the twenty-first century. Journal of European Public Policy, 26(8), p. 1113-1133. https://doi.org/10.1080/13501763.2019.1569711

Hungarian Presidency Council of the European Union (2024): PROGRAMME OF THE HUNGARIAN PRESIDENCY OF THE COUNCIL OF THE EUROPEAN UNION IN THE SECOND HALF OF 2024. Retrieved from: https://wayback.archive-it.org/12090/20250412082714/https://hungarian-presidency.consilium.europa.eu/media/32nhoe0p/programme-and-priorities-of-the-hungarian-presidency.pdf [last accessed on 11.09.2025].

Ivan, P. (2019): Responding to cyberattacks: Prospects for the EU Cyberdiplomacy Toolbox. Brussels, European Policy Centre. Retrieved from: https://www.epc.eu/en/publications/Responding-to-cyberattacks-EU-Cyber-Diplomacy-Toolbox~218414 [last accessed on 17.04.2025].

Kasper, A./Osula, A.-M./Molnár, A. (2021): EU cybersecurity and cyber diplomacy. In: IDP: Revista de Internet, Derecho y Política, 34(1), p. 1-15. Retrieved from: https://doi.org/10.7238/idp.v0i34.387469.

Kasper, A./Vernygora, V. (2021). The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? Cuadernos Europeos de Deusto 65. Bilbao, Instituto de Estudios Europeos, p. 29-71. Retrieved from: https://doi.org10.18543/ced-65-2021pp29-71

Kuckartz, U. (2014): Qualitative Text Analysis : A Guide to Methods, Practice and Using Software, 3. Basic Concepts and the Process of Qualitative Text Analysis p. 54-77 Los Angeles, SAGE Publications, Limited ProQuest Ebook Central. Retrieved from: https://ebookcentral-proquest-com.uaccess.univie.ac.at/lib/univie/detail.action?docID=1633856.

Latici, T. (2020): Understanding the EU's approach to cyber diplomacy and cyber defence. Retrieved from: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651937 [last accessed on 14.07.2025]

Leeson, S.S. (2022): Dutch ruling party calls for Russian hackers to be included on sanctions list. Euractiv. Retrieved from: https://www.euractiv.com/short_news/dutch-ruling-party-calls-for-russian-hackers-to-be-included-on-sanctions-list/ [last accessed on 15.09.2025]

Moret, E./Pawlak, P. (2017): Brief 24: The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime? European Union Institute for Security Studies (EUISS). Retrieved from: https://data.europa.eu/doi/10.2815/399444

Moravcsik, A. (1998): Introduction: The Choice for Europe. In: The Choice for Europe: Social Purpose and State Power from Messina to Maastricht. London, Routledge, p. 1-18. Retrieved from: https://doi.org/10.4324/9781315072258

Poli, S./Sommario, E. (2023): The Rationale and the Perils of Failing to Invoke State Responsibility for Cyber-Attacks: The Case of the EU Cyber Sanctions. In: German Law Journal, 24(3), p. 522-536. Retrieved from: https://doi.org/10.1017/glj.2023.25.

Riordan, S. (2018): The Geopolitics of Cyberspace: A Diplomatic Perspective. In: Brill Research Perspectives in Diplomacy and Foreign Policy, 3(3), Leiden, Brill, p. 1-84. Retrieved from: https://doi.org/10.1163/24056006-12340011.

Rosamond, B. (2005): The uniting of Europe and the foundation of EU studies: Revisiting the neofunctionalism of Ernst B. Haas. In: Journal of European public policy, 12(2), p. 237-254. Retrieved from: https://doi.org/10.1080/13501760500043928.

Sachs, A./Schmalfeldt, I./Zettl-Schabath, K. (2024): European Repository of Cyber Incidents, Research Paper 2: Right thoughts, right words, right actions? The EU's application of the Cyber Diplomacy Toolbox. Retrieved from: https://eurepoc.eu/wp-content/uploads/2024/02/Right-Thoughts-Right-Words-Right-Actions-February-2024.pdf [last accessed on 14.04.2025].

Štitilis, D./Pakutinskas, P./ Malinauskaite, I. (2016): EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. In: Security Journal, 30(4), London, Palgrave Macmillan UK, p. 1151-1168. Retrieved from: https://doi.org/10.1057/s41284-016-0083-9

Stolton, S. (2021): EU must deter cyber attacks against 'essential services,' internal documents say. Retrieved from: https://www.euractiv.com/news/eu-must-deter-cyber-attacks-against-essential-services-internal-documents-say/ [last accessed on 15.09.2025].

Swedish Presidency of the Council of the European Union (2023): sweden2023.eu. Retrieved from: https://wayback.archive-it.org/12090/20231020073516/https://swedish-presidency.consilium.europa.eu/en/ [last accessed on 08.09.2025].

Tonra, B. (2015): Europeanization. In: Joergensen, K. E./Aarstad, A. K./Drieskens, E./Laatikainen, V. K./Tonra, B. (Eds.): The SAGE Handbook of European Foreign Policy. London, SAGE Publications Ltd., p. 182-195. Retrieved from: https://doi.org/10.4135/9781473915190.

Wong, R./Hill, C. (2011): National and European Foreign Policies: Towards Europeanization. (1st ed.). Oxford, Routledge. Retrieved from: https://doi.org/10.4324/9780203816035.

Abbreviations and Software

The graphs were created using the Mermaid Graph tool.

Spellchecking was performed using the Microsoft Word integrated spellchecker, as well as the DeepL Write spellchecker.

EU European Union

CFSP Common Foreign and Security Policy

TEU Treaty on European Union

TFEU Treaty on the Functioning of the European Union

EEAS European External Action Service

EUMS INT European Union Military Staff Intelligence

INTCEN EU Intelligence and Situation Centre

CSIRTs Computer Security Incident Response Teams

EC3 European Cybercrime Centre

ENISA European Union Agency for Cybersecurity

CERT-EU Computer Emergency Response Team for the EU

EUIBAs EU Institutions, Bodies and Agencies

OSCE Organization for Security and Co-operation in Europe

UN United Nations

NATO North Atlantic Treaty Organization

NIS-2 Network and Information Security Directive 2

QMV Qualified Majority Voting

ICT Information and Communication Technology

EU-CyCLONe EU Cyber Crises Liaison Organisation Network