universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„European Integration Without Crisis? Discourses of Securitisation, Convergence and Deterrence in the Evolution of the EU Cyber Crisis Management Regime. "

verfasst von / submitted by

Aaron Schilhan, BA

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

Master of Advanced International Studies (M.A.I.S.)

Wien 2022 / Vienna 2022

Studienkennzahl lt. Studienblatt Postgraduate programme code as it appears on the student record sheet:	A 992 940
Universitätslehrgang lt. Studienblatt Postgraduate programme as it appears on the student record sheet:	Internationale Studien / International Studies
Betreut von / Supervisor:	Professor Markus Kornprobst, M.A., Ph.D.

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

Abstract

In recent years an accelerated process of European integration in the field of cyber crisis management can be constituted. The European Union (EU) has established a great number of agencies, cooperation structures and crisis management mechanisms to deal with the transboundary nature of modern crisis. Neofunctionalist and liberal intergovernmentalist approaches are increasingly relying on crisis as a catalyst for institutional change. However, to date there has never been a large-scale cybersecurity incident that holds to the definition of a cyber crisis. This thesis will trace European integration in the field of cyber crisis management by applying discursive institutionalism (DI) to explain European integration in the absence of crises. By establishing a causal mechanism based on the discourses of *securitisation, convergence* and *deterrence*, the integration dynamics will be traced that led to the existing EU cyber crisis management regime (CCMR). By examining the 'EU Cybersecurity Strategy', the 'NIS Directive', the 'Blueprint' and the 'Cyber Diplomacy Toolbox' this thesis will show that a philosophical discourse of *securitisation* initiated European integration, which was then driven by programmatic discourses on *convergence* and *deterrence*, and incomplete institutional reform due to conflicting national and supranational discourses and incompatible cognitive and normative ideas.

Abstrakt

In den letzten Jahren hat sich der Prozess der europäischen Integration im Bereich des Cyber-Krisenmanagements beschleunigt. Die Europäische Union (EU) hat eine Vielzahl von Agenturen, Kooperationsstrukturen und Krisenmanagementmechanismen eingerichtet, um mit dem grenzüberschreitenden Charakter moderner Krisen umzugehen. Neofunktionalistische und liberale intergouvernementalistische Ansätze setzen zunehmend auf die Krise als Katalysator für institutionellen Wandel. Bislang hat es jedoch noch nie einen großflächigen Vorfall im Bereich der Cybersicherheit gegeben, welcher der Definition einer Cyberkrise entspricht. In dieser Arbeit wird die europäische Integration im Bereich des Cyber-Krisenmanagements nachgezeichnet, indem der diskursive Institutionalismus (DI) angewandt wird, um die europäische Integration in Abwesenheit einer Cyberkriese zu erklären. Durch die Etablierung eines kausalen Mechanismus, der auf den Diskursen der *Versicherheitlichung*, *Konvergenz* und *Abschreckung* basiert, wird die Integrationsdynamik nachgezeichnet, die zum bestehenden EU-Cyberkrisenmanagement-Regime (CCMR) geführt hat. Durch die Untersuchung der "EU-Cybersicherheitsstrategie", der "NIS-Richtlinie", des "Blueprints" und der "Toolbox für Cyberdiplomatie " wird diese Arbeit zeigen, dass ein philosophischer Diskurs der *Versicherheitlichung* die europäische Integration einleitete, die dann durch programmatische Diskurse über *Konvergenz* und *Abschreckung* und unvollständige institutionelle Reformen, aufgrund widersprüchlicher nationaler und supranationaler Diskurse und unvereinbarer kognitiver und normativer Ideen vorangetrieben wurde.

On my honour as a student of the Diplomatic Academy of Vienna, I submit this work in good faith and pledge that I have neither given nor received unauthorized assistance on it.

Aaron Schilhan

Table of Contents

Introduction

Since the turn of the century policy makers within the European Union (EU) became aware of the increasing vulnerability of European societies to cyber incidents due to their growing dependence on information and communications technologies (ICTs). While more sectors become digitalised, cyberspace evolves to be an increasingly contested domain as cyberattacks continue to surge and are increasingly aimed at critical infrastructures. Cyber crises, as the most severe form of cybersecurity incidents are conceptualised to potentially represent an existential threat to the European economy, its fundamental values and its societies. To cope with these challenges a fragmented network of cyber crisis actors, cooperation structures and crisis management mechanisms was established by the EU. Spread across four cybersecurity communities, EU capacities were created to support Member States in managing the transboundary nature of cyber crisis. This patchwork of cyber crisis management capacities is the result of an accelerated process of EU integration in the field of cyber crisis management, that can be observed in the recent years. Under the von der Leyen Commission, strategic transboundary crisis management has become a clear priority and efforts to become a unified and capable cyber crisis management actor have continuously developed.

While European integration in that field can clearly be observed, explanations on why an EU cyber crisis management regime (CCMR) developed and why it took the particular shape it has today, are inexistent. The literature on European integration is currently most adamant on the explanatory power of crises causing institutional change (Biermann et al., 2019; Hooghe & Marks, 2019; Lefkofridi & Schmitter, 2015). Some authors develop this ideas by combing neofunctionalist and liberal intergovernmentalist approaches to construct a cyclical process of 'failing forward' (Bergmann & Müller, 2021; Jones et al., 2021; Lavenex, 2018). In this view, crises cause the EU institutions to instigate institutional change to cope with their impacts on a supranational level. Institutional reform is however often incomplete due to intergovernmental bargaining, which causes dysfunctional structures that are susceptible to crisis and in turn cause the process to start over. European integration is thus a combination of supranational agency that drives institutional reform, which is however incomplete due to divergences in national preferences.

While this approach is able to trace the EU's integration process in many domains, it is incapable for doing so in the field of cyber crisis management. The simple reason being that there has never been a cyber crisis. No incident that occurred within the European Union ever holds up to the currently employed definition of a cyber crisis. A cyber crisis according to the

EU must include the incapability of a Member State to manage crisis on its own, or the fact that two or more Member States are affected. This begs the question: why was there substantive integration in the field of cyber crisis management in the absence of a cyber crisis?

This thesis seeks to answer this question and overcome the shortcomings of the 'failing forward' approach. It will do so by applying discursive institutionalism (DI) to the process of European integration and explain how institutional change is possible without the necessity of incurring crises. The main argument will be that European integration in the field of cyber crisis management was the result of discourses of *securitisation*, *convergence* and *deterrence.* Through a discourse of securitisation, the idea was established that a potential cyber crisis would have such a devastating impact on the EU and its Member States, that capabilities for cyber crisis management must be established. What then follows are discourses of convergence and deterrence introducing ideas on how to manage crisis in cyberspace. While convergence represents the idea that cyber crises are best managed at the supranational level to cope with the transboundary nature of cyber crisis, deterrence states that comprehensive cyber crisis management can only be accomplished by introducing proactive strategies to reactive ones due to the peculiarities of cyberspace. Integration dynamics are furthermore perpetuated by incomplete institutional reform that is the result of conflicting national and supranational norms, as well as incompatible cognitive and normative ideas. A causal mechanism is established, that constitutes a cyclical form of integration leading to institutional layering. By applying a discursive approach, it is possible to explain European integration without the necessity of a crisis. Integration in the field of cyber crisis management can thus be observed, as the securitisation discourse contains a conceptualisation of a cyber crisis that introduces the necessity for cyber crisis management. I will develop this argument and test it empirically in two parts.

Part I will introduce the explanatory power of discourses in institutional change, examine the peculiarities of cyberspace and cyber crisis and contextualise them in the discourses of securitisation, convergence and deterrence. By doing so, Part I will introduce a causal mechanism for European integration, which is based on discourses and is not reliant on the presence of crises. Part II will then test this causal mechanism by examining key steps of European integration in the field of cyber crisis management. The *Cybersecurity Strategy* of 2013, the *NIS Directive* of 2016, the *'Blueprint'* of 2017 and the *Cyber Diplomacy Toolbox* of 2017 will be analysed in respect to the discourses of securitisation, convergence and deterrence,

and their underlying causal mechanism. It will furthermore discuss the future of the EU's CCMR and discuss the EU as a cyber crisis manager.

This paper will contribute to the existing literature by introducing a causal mechanism that can explain European integration without the necessity of a crisis. It will furthermore highlight the explanatory power of discourses in institutional change and propose an alternative for neofunctionalist and liberal intergovernmentalist approaches. The case study will show that European integration in the field of cyber crisis management is one of underlying ideational continuity on a philosophical level, which has been shaped by ideas of how to manage cyber crisis on a programmatic level. Further integration is then triggered by incomplete institutional reform due to conflicting national and supranational discourses on the functionality and the legitimacy of existing and newly introduced structures. The next chapter will present a literature review to examine existing accounts of EU cyber crisis management and European integration.

Literature Review

Most of the current academic literature on EU crisis management is primarily interested in the EU's capabilities to manage transboundary crisis. Cyber crisis management can be understood as a subset of generic transboundary crisis management, which renders this strand of literature highly relevant. Ansell et al. (2010) in their article deal with the implications of the transboundary nature of a crisis. They conceptualise a transboundary crisis as one that can traverse geographical distances, policy boundaries and do not have a fixed starting or end point. They then argue that transboundary nature of crisis results in the major political administrative challenges of coping with uncertainty, providing surge capacity, organizing a response and communicating with the public. They then propose 'boundary-spanning' crisis management capacities. The conceptualisation of transboundary crisis was ground-breaking as it introduced its borderless nature and proposed the necessity of international cooperation in their management.

Building on this article, Boin, Rhinard, and Ekengren (2014) take stock of the EU's evolving capacities to manage transboundary crisis. They examine EU capacities in the fields of managing borders, epidemics, critical infrastructures, financial crisis, and countering terrorism. They find there is no comprehensive 'boundary-spanning' crisis management framework in place. They rather deem the EU's transboundary crisis management capacities to resemble a fragmented network, which is only slowly evolving. They go on to propose

reasons for the lack of integration. First, they name a lack of clear ambitions. Until the time of the article, there has been no clear call for a systematic development of transboundary crisis management capacities, and crisis has been subsumed under a national security discourse. Second the EU's capacity to adapt to crisis hinders an overarching institutionalisation of transboundary crisis management. Crisis management policies thus far had evolved as a response to an incurring shock, and the EU's adaption to the shocks had been perceived as functioning and legitimate. The authors conclude that the reluctance of Member States to confer more powers to the EU institutions renders the prospect of a systematic institutionalisation of transboundary crisis management unlikely. This account is interesting as it introduces the EU as a fragmented transboundary manager, that lacks substantive capability development in the field due to a lack of supranational ambition and competing national discourses.

Boin, Busuioc, and Groenleer (2014) further build on this work and use the taxonomy of governance modes introduced by Provan and Kenis (2007). The EU in their account represent a network mode of governance, characterised by its fragmented nature. The authors go on compare this mode to a more hierarchical, lead-agency mode to deduct their possible strengths and weaknesses. These are measured through the dimensions of *sense making, coordination* and *legitimacy,* and come from the main challenges of a transboundary crisis. The main argument of the article is that while a network model has certain strengths, as the reliability of information through a redundancy in information sources and an increase in legitimacy in the context of the EU, a lead-agency model can increase responsiveness in a coordinated and timely manner. The authors conclude that the EU has over the years introduced new crisis management capacities, without a general blueprint that would introduce harmonised structures, propelled by a lack of supranational incentive and intergovernmental bargaining that led to lowest-common-denominator solutions. Introducing hierarchical elements of a lead-agency model, generic instead of sectoral capacities and a systematic approach to integration in the field, would increase the EU's capacities to manage transboundary crisis. This article is relevant as it introduces the benefits of introducing more hierarchical and generic crisis management capacities in the EU. It again shows that the EU's development in becoming a capable transboundary crisis manger is hindered by the lack of a blueprint and lowest-common-denominator solutions.

Backman and Rhinard (2018) go on to take stock of the EU's capacities for transboundary crisis management. They include in their work new foci for analysing

transboundary management capability, determined by the evolving crisis management literature. The literature currently established seven dimensions of managing transboundary crisis: detection, sense-making, decision-making, coordination, meaning-making, communication, and accountability. The authors then examine the existing EU capacities of transboundary crisis management, and group them in these dimensions. They show that the EU has most of its capacities for managing crisis in the detection/sense-making categories. Integration in this dimension is evolving more rapidly as Member State do not oppose these mainly administrative capacities that do not infringe with their national sovereignty. Decision-making and coordination show opposite dynamics. This paper examines the EU's capability to manage transboundary crisis by grouping existing capacities into the dimensions of transboundary crisis management. In the same manner as previous accounts, the authors find that most of the crisis management capacities of the EU are sectoral and incentives for overarching approaches are stagnating. Their contribution is relevant to this paper, as it clearly depicts discourses of national sovereignty to infringe with comprehensive European integration in the field of cyber crisis management.

Boeke (2018) contributes to the cyber crisis management literature, as he analyses different approaches of cyber crisis management by employing the previously used taxonomy of modes of governance to the Czech Republic Denmark, Estonia, and the Netherlands. He analyses the public-private partnerships of the four countries and categorises them into the slightly amended modes of participant-governed networks, lead-organization-governed networks, and a network administrative organization. He finds that while the governance model of Estonia and the Czech Republic to be closest to a network-administrative model, the Netherlands resemble a participant-governed model, and Denmark a lead organization model. Boeke contributes to the literature as he stresses the importance of public-private cooperation in the domain of cyber crisis management and defines cyber crisis management as a subset of generic crisis management, related to the increasing digitalisation of different sectors of modern society. The importance of the perception of cyberspace as a strategic environment is furthermore stressed. Even though it is not the focus of analysis, Boecke points out that the examined countries have different conceptualisations on what cyber crises are and apply different approaches to managing them. This is important as I will argue that the discourses of cyber crisis management are derived from a conceptualisation of cyberspace and cyber crisis.

While not explicitly examining transboundary-, or cyber crisis management, Bergmann and Müller (2021) wrote an article on the evolution of the EU's crisis management within its

Common Security and Defence Policy (CSDP). By examining the Civilian CSDP Compact (CCC) and the European Peace Facility (EPF), the authors find a cyclical integration process that follows the 'failing forward' rational. The argument they present is that integration in the CSDP's crisis management is caused by a crisis, which is followed by partial institutional reform that leads to policy feedback, and experiential learning. This process then causes incomplete reforms to address previous shortcomings, which lead to further crisis and drive the integration process in a cyclical manner. Their integrated theoretical approach of combining supernationalist agency, institutional learning and Member State bargaining is able to capture integration dynamics in the field of the CSDP's crisis management. This approach is however heavily reliant on the incurrence of a crisis to drive European integration, which cannot be observed in the integration of cyber crisis management. This paper and the failing forward approach in general however are very relevant to this thesis, as they introduce a cyclical form of integration that is driven by incomplete institutional reform. This argument will also be developed in this thesis, however on the basis of discourses instead of crisis. Furthermore, this article leads us to the literature on European integration in the cyber domain.

Another strand of academic literature, relevant to this thesis is concerned with the integration processes of the EU within the cyber domain. Still very much related to EU capabilities, Fahey (2020) in her work examines the EU as a cyber security actor. By examining the evolvement of EU cyber law, she traces the institutionalisation in the cyber domain and gives an account on EU actorness. She finds that the EU lacks sufficient institutions and agencies to be considered a capable cybersecurity actor. She makes the argument that the EU's weak actorness stems from partial and fragmented institutionalisation in the cyber domain that can inter alia be attributed to diverging definitions of cybersecurity. Fahey's contribution to the literature prescribes the EU weak actorness as a cybersecurity actor and points to the importance of standardised conceptualisations in the process of European integration, which is represented in this paper through the discourse on *convergence*.

Carrapico and Barrinha (2017) also examine the EU as an evolving (cyber-)security actor and adopt coherence as a measurement of actorness. The authors first trace convergence as an evolving concept within the EU in the field of cybersecurity and then examine the coherence of the EU's cyber policy. Convergence is then measured twofold. Once through examining institutional coordination, and secondly through analysing a shared understanding of the security environment. The authors conclude that the EU has the ambition of being a coherent cybersecurity actor, but the fragmentation is still impeding its actorness, as is the

Member States' reluctance to confer more powers to the supranational level. Their article contributes to the literature as they depict the evolvement of an EU cybersecurity actorness, related to the rising complexities of the modern security environment. They then introduce convergence as means to deal with this complexity and measure the EU's actorness in relation to its level of convergence. The author's account is central for establishing the convergence discourse in this thesis, which is an incremental part of the causal mechanism explaining European integration in the field of cyber crisis management.

Another essential discourse in the causal mechanism of this thesis is presented by Christou (2019). In his article he examines the evolving of the securitisation of cyberspace within the EU. Tracing the securitisation discourse over time, the author finds that network and information systems are framed to be increasingly vulnerable. While the emerging securitisation discourse was in its initiation shaped by economic motives, it evolved to include a substantial threat to European societies and European values. A collective securitisation thus happened, that positions the EU as a cybersecurity actor to deal with the increasing vulnerabilities emerging through digitalisation. The securitisation discourse is then shown to be the basis on which the EU develops new institutional structures to deal with the threats and dangers in cyberspace. Linking the cyber domain to questions of security allows to keep the policy field at the top of the EU's agenda and leads to the willingness of Member States to adopt new law in the policy field. This contribution is crucial to this thesis, as it not only constructs the securitisation discourse within the EU but examines its impact on existing institutional structures. It furthermore shows that discourses are not static and that a change in discourse can cause institutional change.

Carrapico and Farrand (2020) go on to apply the theory of discursive institutionalism (DI) to European integration. They examine the impact of the COVID 19 Pandemic on the trajectory of EU cybersecurity policy by examining its impact on the discourses surrounding it. They first show, that the role of social media platforms in disseminating disinformation has changed the cybersecurity discourse from one that sought to include private companies as much as possible in EU policy making, to one that promotes stronger oversight over them. The authors conclude that the COVID-19 pandemic, while increasing societies dependency on ICTs and thus creating more vulnerabilities, has not caused a change in discourse, but rather enforced it. The pandemic has led to a stronger and more widespread belief that private companies must be subjected to stronger supervision in the context of spreading disinformation. This article is very central to this thesis as DI is the chosen approach to examine European integration in the

field of cyber crisis management. DI lays the groundwork for explaining how discourses can lead to institutional change. In the context of this paper, it furthermore shows that a crisis, as the COVID-19 pandemic, does not necessarily cause institutional change and European integration.

The literature on EU cyber crisis management and European integration in the cyber domain gives us several thoughts. Firstly, cyber crises, as transboundary crises pose a unique set of political-administrative challenges. Related to the borderless nature of cyberspace, managing cyber crises effectively must include international cooperation. Secondly, the EU thus far approached these challenges by introducing network type governance, that is fragmented across policy areas. However, transboundary crisis management requires strong convergence of capabilities and situational awareness. The EU is thus prescribed limited capabilities due to weak institutionalisation and a lack of hierarchical structures. Thirdly, European integration is often approach by a 'failing forward' approach, that relies on the necessity of a shock or crisis and incomplete institutional reform that perpetuate integration. Fourth, discourses show great potential for explaining European integration. Especially discourses on securitisation and convergence are shown to facilitate European integration and cause institutional change.

What is missing however is the establishment of a causal mechanism, that explains European integration without the necessity for a crisis and applies this mechanism to the European integration in the field of cyber crisis management, in relation to the unique challenges of transboundary crisis management. I seek to close this gap by posing the questions of why European integration in the field of cyber crisis management happened and, how the existing crisis management regime came to be. To answer these questions, I proceed as follows. The first chapter of Part I will introduce ideas and discourses as the drivers for institutional change. I will argue that institutional change happens when underlying philosophical ideas about how the world works change or if programmatic ideas of how to deal with defined problems are no longer perceived as functional or legitimate, in relation to the overarching philosophies and normative constellations. The second chapter goes on to conceptualise cyberspace and cyber crises, to frame the existing discourses on cyber crisis management. The third chapter will then define three salient discourses on cyber crisis management and introduce a causal mechanism for institutional change. Part II of this thesis will go on to examine this causal mechanism in the light of the European integration process in the field of cyber crisis management.

Part I - Why Discourses Matter

Discursive approaches have thus far not gained much attention in the academic literature on European integration. The literature review on transnational crisis management and European integration has however hinted at the great potential of discourses to explain institutional change. A discursive approach can most importantly tend to the shortcomings of the 'failing forward' approach and its heavy reliance on incurring crisis for explaining European integration. The following chapter will thus introduce discursive institutionalism (DI) to answer the questions of why integration can be observed without a crisis and how the currently existing structures came to be. First, DI and its basic assumptions will be outlined. By applying a discursive understanding on institutions, interests and norms, it will be shown that they are dynamic constructs that can be subject to change at any given time. Secondly, ideas will be conceptualised, to introduce an understanding of how ideas, through discursive iteration, cause institutional change. By introducing a matrix of ideas, it will be shown that institutional change occurs as overarching philosophies of how the world works change, or if programmatic ideas of how to interact with this world are perceived to no longer be functional or legitimate, in relation to philosophies and normative constellations. I will then deduct a causal mechanism, that institutional change caused by discourses may lead to incomplete institutional reform through a conflict of programmatic ideas with normative constellations. The incomplete institutional structures are then subject to change again, if they are no longer perceived to be functional or legitimate.

Chapter 1: Discourse and Institutional Change

As previously discussed, discourses show to have great potential in explaining institutional change. This potential was recognised by Schmidt (2008) who went on to elaborate a fourth 'new institutionalism' a discursive institutionalism (DI). Her approach introduces a discursive understanding to institutional change, which separates it from other institutionalist approaches as historical institutionalism (HI), rational choice institutionalism (RI), and sociological institutionalism (SI). The basic assumption that separates DI from the other approaches is the dynamic nature of institutional structures, interests and norms. I will now introduce DI in distinction to the other three new institutionalisms to elaborate how ideas shape institutions and how discourses shape ideas.

Institutions, ideas and discourses

In a constructivist manner and in line with DI, institutions are to be defined as contingent structures that are constituted by actors. Institutions are a "[...] structure, or code, or regulated pattern of behaviour which becomes 'legitimate' and 'functioning' within a social context, and which is relatively stable and persistent over time." (Lanzara, 1998, p. 1). Functionality in this sense can be defined as an institution's ability to serve the interest of the respective actors, while legitimacy is defined as the adherence of institutions to the normative constellation of an actor. As institutional structures must continuously be rearticulated, they can be subject to change at any given time. In relation to applied definition, institutions change, once they are perceived to be incapable of effectively promoting an actor's interests or as they are perceived to be incompatible with an actor's norms. In that manner DI breaks with the logic of statically evolving institutions based on path dependency, as proposed by HI.

Interests in DI, follow the same logic and are in opposition to RI neither eternal, nor objective. Interests are to be understood as subjective ideas, that must be continuously rearticulated. In the same manner as institutions, they may change at any given time. As actors constitute institutions, a change in interests or ideas of actors may thus lead to institutional change. The same logic applies to norms. Different than in SI, norms as subjective ideas and are continuously rearticulated, and are the product of intersubjective ideational constructions. Norms can change over time but must also be reaffirmed to continue as a part of an actors' normative constellation. Institutional change in DI is thus not dependent on the static path dependent evolvement of institutional structures, nor on predetermined interest or on eternal norms (Schmidt, 2008).

Institutional change is then dependent on the interests and norms of the actors constituting them. As ideas change, the structures of a given institution change. Discourses in this regard are able to explain why and how ideas change. Discourses, as conceptualised in DI, are the articulation of ideas. Ideas are discourses' substantive content, and discourses are the relational act of expressing ideas, in any shape or form of communication. On the substantive level, discourses can change institutional structures by introducing ideas that can alter or replace existing ideas. Existing ideas may be altered or replaced by new ones, as they are show greater potential in promoting an actor's interest or adhere better to normative constellations. The articulation of ideas can thus alter existing ideas in the institutional structure due to their perceived 'functionality' or 'legitimacy'.

Additionally, to the importance of what is communicated (ideas), lies the importance of the context and the agent who is communication its ideas (agency). On the agency level discourses can change existing ideas within an institution if an actor with strong agency communicates ideas. An actor can in that manner change ideas of other actors as she is perceived as credible and thus lead to institutional change. An actor can furthermore possess strong agency by her positioning in the institutional structures. A policy maker at a high level has stronger agency than an expert in an advisory role. Some institutional structures also introduce the possibility of veto players, which in this context have very strong agency. The context of the existing intuitional structures, as well as the agent conducting the discourse play an important role in institutional change (Schmidt, 2008, pp. 309–313).

What now follows is a relationship between institutions, ideas and discourses. Discourses, depending on content and the agency may change the normative or interest based ideas of given actors. A change in ideas will then lead to a change in the institution that is constituted by its actors. I will now introduce a matrix of ideas to explain how

A Matrix of Ideas

As we have previously discussed, interests and norms are both to be considered subjective ideas. As interests are heavily related to rationalist approaches, I will reframe them as cognitive ideas, complementing normative ideas. Furthermore, not all cognitive and normative ideas have the same quality. They rather come in three different tiers, defined by their level of generality, which I will introduce now.

The first, most general level of ideas is the level of core philosophies or worldviews. They are the underlaying ideas that determine the very way in which an actor perceives the world. Ideas at the philosophy level are considered background ideas, as they are often taken for granted, and the least susceptible to change. This overarching layer are fundamental ideas from which the other levels of ideas are derived from. The second, more specific level is a programmatic level of ideas. Programmatic ideas are formed as based on the underlying philosophy. They define problems, possible solutions and set strategic guidance. Programmatic ideas, based on underlying philosophies, shape the possibilities of how a defined issue can be resolved. The third tier are policy ideas. These ideas contain information of how defined problems are approached. They are to be seen as the result of the two other levels and constitute, together with the programmatic level the foreground ideas.

We can now link the distinction between cognitive and normative ideas with the level of generality. Cognitive ideas at the philosophy level constitute an actor's perception of the world or in other words, what is. On the programmatic level cognitive ideas defines what needs to be done in accordance with problems derived from the philosophy level. On the policy level, cognitive ideas are then what will be done to address to problems defined at the programmatic level. On this level, 'functionality' is assessed, based on an ideas capability to resolve previously defined problems. On the normative side, ideas attach value and produce legitimacy. Normative ideas at the philosophical level make up the underlying normative constellation of an actor. Normative ideas on the programmatic level define what should be done in relation to an actor's norms. On the policy level, normative ideas define whether the proposed action is good or bad, determined by its adherence to the underlying normative constellation. On this level, an ideas legitimacy is decided (Schmidt, 2008, pp. 306–307).

By distinguishing between cognitive and normative ideas and introducing three tiers of generality an ideas matrix is established, which allows us to examine more precisely how institutional change comes about. We have established thus far that discourses may change ideas, that in turn cause institutional structures to change. By inferring from the ideas matrix, we can now say that discourses can change an actor's cognitive or normative ideas on a philosophical, programmatic, or policy level. On the philosophical level, institutions change as the worldview or normative constellation of an actor is altered. On the programmatic level, institutions change as new problems and means to address them are defined by ideas on what needs to be done in relation to an actor's worldview and what should be done in relation to an actor's normative constellation. On a policy level, institutions change as the perception of ideas to be functional, in relation to what needs to be done, or to be legitimate, in relation to what should be done, changes. Institutional change thus happens as existing structures are deemed to be either dysfunctional or illegitimate. Discourses may alter cognitive and normative ideas at all different levels of generality and thus cause institutional change.

We have now begun to construct a causal mechanism for European integration. As a last step we need to account for incomplete institutional change in the spirit of the failing forward approach. There are two reasons for the introduction of incomplete institutional reform. The first explanation is diverging or conflicting discourses between the EU institutions and the Member States. On the one hand Member States might not share the same overarching cognitive philosophy as the EU institutions, which would lead to a difference in defining problems and introducing functional solutions. A legislative act proposed by the EU could be

in line with its underlaying worldview and perfectly fit the defined challenges to be addressed. If a Member States does however have different philosophical or programmatic ideas, the proposed legislative act would be perceived as dysfunctional from the get-go as it does not relate to a Member State's defined problems or worldview. On the other hand, Member States have normative constellations that are not congruent with the constellation of EU institutions. While a proposed legislative act may be in line with the EU's norms, it may very well conflict with national norms. A prominent example is the norm of national sovereignty.

A second reason for the introduction of incomplete institutional change is the conflict between the cognitive and normative ideas. A cognitive idea at the policy level may perfectly address the problems defined at the programmatic level and be in line with the underlying worldview. The same idea may however conflict with the underlying normative constellations. An idea could be the perfect solution for a defined problem, but still never be introduced as it conflicts with existing norms. The idea would be deemed functional but illegitimate and not lead to institutional change. In that way, the introduction of a complete institutional reform may be hindered by its conflict with existing norms, be amended and thus lead to incomplete institutional reform. Both, a conflict between supranational and national ideas and a conflict between cognitive ideas and normative constellation may thus constitute incomplete structural reform, leads to further integration. At this point, it is important to notice, that integration in the context of the EU often follows the logic of institutional layering. New institutional structures are added to existing ones in order to reshape behaviour. This allows for institutional change, without the need to abolish old rules of behaviour. Institutional layering often happens in environments with strong veto powers, as is the case for some of the EU's policy fields as the CFSP/CSDP. Institutional layering is however not incapable of achieving substantial change. Adding new layers can fundamentally alter existing ideas that are constitutive of the institutional structure (Mahoney & Thelen, 2010).

We can now establish a causal mechanism to explain European integration. Institutional structures can be changed as discourses alter an actor's cognitive or normative ideas on a philosophical, programmatic, or policy level. Institutional change may however be incomplete due to conflicting supranational and national discourses, or due to the incompatibility of a complete reform with existing normative constellations. As incomplete reform is introduced, new discourses arise, deeming existing institutional structures either dysfunctional or illegitimate. This starts the process anew and leads to further integration in the form of institutional layering. In order to test causal mechanism in European integration in the field of

cyber crisis management, it is necessary to define salient discourses that initiated and drive this process. The next chapter will thus introduce a conceptualisation of cyberspace and cyber crisis to infer salient discourses that drove European integration in the field of cyber crisis management.

Chapter 2: The Particularities of Cyberspace and Cyber Crisis

In the academic literature and in national cybersecurity strategies, cyberspace is often referred to as a global common to which all governments have legal access comparable to airspace, the high seas, or outer space. Another way is to frame cyberspace in a strategic way, as the fifth domain of warfare. These conceptualisations are however flawed, as cyberspace, in opposition to the other domains is entirely humanmade. What follows is that not only, it is unique as a domain, but also that conventional strategies do not apply to it, due to this uniqueness (Barrinha & Renard, 2017). By examining the peculiarities of cyberspace, we understand the arising discourses of cybersecurity and strategic cyber crisis management. In the following I will show how the uniqueness of cyberspace causes a securitisation discourse on a philosophical level and a strategic discourse on deterrence on at programmatic level.

Conceptualising Cyberspace

Cyberspace is a product of what may be called the 'age of information'. This terminology was introduced in the mid-1990s to describe the great and rapid advancements in the field of information and communications technologies (ICTs). It was also chosen to indicate a new era of human interaction, which is clearly distinct from any period before. The development of the personal computer and its integration into a world-wide network of networks, drastically changed the way our relationship with information. Through cyberspace, information has become more accessible, decoupling accessibility of information from its geographic location. Cyberspace has furthermore made information more available. One source of information be shared infinitely and be retrieved at the same time by multiple users. The speed in which information can be accessed has also augmented tremendously, and increasingly more people can afford to access information, as the necessary technology becomes cheaper over time. Cyberspace as the product of the information age has thus made information more accessible, available, affordable and increased its speed. The evolution of cyberspace has not only created a new realm of human interaction, but due to its nature has its own particularities for said interaction, that will now be discussed.

The first implication of an emerging cyberspace is a drastic empowerment of the individual. A single actor is now able to access, process, and generate information at a very low threshold. This increasing low cost of entry leads to a great diversification of actors. Anyone can potentially become an actor in cyberspace. The individual becomes empowered vis-à-vis the state. This empowerment does not only happen because of the relational increase in personal accessibility of information, but also due to the nature of cyberspace itself. Cyberspace as an information technology network is ideally structured anarchically. This means there is neither physical centre in which all the connections come together, nor a centralised authority. The network linkages may emanate from different central sources but are not dependent on that source to be connected to one another. Additionally, there is no hierarchical superior power in cyberspace that can enforce a certain behaviour. Cyberspace is anarchical in nature, which means power cannot be monopolised by states as easily as in the physical realm. The individual is thus empowered in relation to the state through its more improved relation to information, and the lack of a hierarchical structure with a central authority.

Secondly, cyberspace is a highly dynamic and malleable terrain. Cyberspace has a physical and a non-physical dimension. One part of the physical dimension is that Cyberspace is manmade. Cyberspace is the connection of physical entities within a network of networks. Its size is therefore related to the number of physical devices connected to it. As a new device accesses cyberspace, the space itself grows. This does not only mean that the number of actors within cyberspace constantly change, but that the physical structure itself changes as well. This malleability is furthermore related to the threats and dangers that are systemic within cyberspace. As the structures of cyberspace constantly change though a physical altering of cyberspace or the evolvement of new technologies, weaknesses of information networks may be exposed. A change in structure can alter the effectiveness of cyber defences, or new offensive capabilities may be developed, that are capable to penetrate these defences. This ultimately means that there are no absolute defensive capabilities in cyberspace.

Thirdly, cyberspace is a borderless terrain of constant contact. Cyberspace for one is borderless in the sense that it has no physical borders. This is especially relevant in the context that it has no national borders. Albeit that the physical part of cyberspace is linked to territoriality, it is sheer impossible to draw these boarders in the non-physical realm. Furthermore, cyberspace is borderless in relation to providing interconnectedness. Actors from all over the globe can interact with each other as if there was no physical distance between

them. This means, that any actor in cyberspace is in constant contact with any potential and every potential adversary. The borderless nature adds to the malleability in that it makes defending in cyberspace more difficult.

Fourthly, attribution poses the biggest challenge in cyberspace. The technical endeavour of attributing cyberattacks to a specific actor is one that is very costly, time-consuming and might not ever be successful. The way in which cyberspace is constructed makes it possible for actors to stay anonymous over long periods of time. Potential adversaries can thus covertly conduct malicious behaviour because they can potentially stay undetected forever (Fischerkeller et al., 2020) What adds to the problem of attribution is that cyberattacks themselves may never be detected. In cyberspace, cyberattacks must be perceived as cyber campaigns, rather than single events. They may stretch over long periods of time, trying to gain a strategic advantage and causing a lot of damage undetected (Harknett & Smeets, 2020). As cyberattacks may never be detected or impossible to attribute to an adversary, holding actors accountable is an extremely difficult endeavour. A way to deal with this problem of uncertainty is political attribution. Political attribution was introduced to bypass the necessity of having absolute certainty of in technical means. In political attribution, the capabilities and likelihood of actors to commit the cyberattack in question are assessed. In this manner, the US and Israel are attributed to be responsible for the attack on Iranian nuclear centrifuges with the malicious Stuxnet computer worm (Interview 5).

Conceptualising Cyber Crises

Cyberspace is thus a highly malleable and borderless terrain that brings systemic and manmade risks. Increased digitalisation and the continuous development of new potentially harmful technologies renders societies more vulnerable. In this context, a cyber crisis is the most drastic incident societies can face and managing them is especially difficult due to the peculiarities of cyberspace. The literature has already dealt with the question of how to conceptualise a crisis in cyberspace (Backman, 2021; Backman & Rhinard, 2018; Boin, Busuioc, & Groenleer, 2014; Prevezianou, 2021). It uniformly agrees that cyber crises are to be understood as version or subcategory of transboundary crisis. In general crisis are defined as severe threats to core values of a society, that require urgent response and carry a substantive amount of uncertainty (Tagarev & Ratchev, 2020). Crisis are then transboundary of nature if they transcend political boundaries of geographic locations and policy areas, as well as stretch over longer periods of time, in which a clear demarcation of a beginning and end is not possible (Ansell et al., 2010). Cyberspace provides additional layers to the definition of a transboundary crisis. First, a crisis

in cyberspace introduces an increase in complexity of a crisis. As cyberspace is borderless and interconnects increasingly many societal domains, crisis become more complex. A vulnerability in one sector may interact with other sectors, causing chain reactions that have great escalatory potential (Backman, 2021). Secondly, crisis in cyberspace may face a vacuum of authority. As cyber crisis management is currently highly fragmented within nations, and even more so across them, even in the context of the EU, definitions of responsibilities may conflict as crisis spread across national borders, or happen in the non-physical, borderless realm of cyberspace (Prevezianou, 2021).

The literature has identified key political-administrative challenges regarding the management of transboundary and cyber crisis: detection, sense-making, decision-making, coordination, meaning-making and accountability. Detection is the challenge of recognising threats as they emerge. In cyberspace, this can be extremely difficult as new technologies constantly evolve and tools of threat detection or horizon scanning may be incomplete. Sense-making is the process of analysing critical information and sharing it to all relevant crisis management actors. Understanding what is going in a situation of crisis is a very hard endeavour, but the process becomes even more complex when a transboundary nature of a crisis is added. Decision-making is concerned with formulating a strategic approach of crisis management, based on the available information. As transboundary crises are often related to an authoritative vacuum, or fragmented and decentralised structures, decision-making is one of the biggest challenges. Coordination of action is furthermore key in this regard. Crisis are needed to be responded to in a timely and coordinated manner to successfully manage them. Identifying key actors and coordinating action between them is thus crucial. Meaning-making is concerned with formulating an account of what happened. The crisis must be elaborated upon to grant legitimacy to the decision-makers. Finally, accountability takes stock of how a crisis was responded to and why these particular means were chosen. This step includes feedback loops and stakeholder dialogues and allows for learning processes (Backman & Rhinard, 2018). These key challenges must be taken on in the effort of managing cyber crisis in a timely and effective manner. Due to the introduced peculiarities of cyber crises, they are conceptualised to be addressed best at an international level. The driving rationale is that through a convergence of structures and situational awareness, the problems of exponential complexity and authoritative vacuum can be mitigated and permits a timely and effective crisis management.

This conceptualisations of cyberspace, cyber crisis, their particularities and their respective political-administrative challenges allows three major conclusions. Firstly, cyberspace has inherent risks and dangers that renders it an increasingly contested space and could potentially cause great damages to societies, as they become more dependent on ICTs. Cyberspace is a borderless and malleable domain in which the individual becomes empowered, and attribution poses a great challenge. Offensive strategies are thus favoured in cyberspace as an absolute defence is impossible, adversaries can potentially stay undetected and may even not fear punishment due to an uncertainty in attribution. Secondly, cyber crises are a transboundary phenomenon, that pose unique political-administrative challenges that are best dealt with internationally. Cyber crises can spread across political boundaries, geographic locations and undefinable periods of time. They furthermore turn exponentially complex as they unfold and may encounter an authoritative vacuum. A convergence of structures and situational awareness allows for a timely and effective cyber crisis management. Thirdly, the peculiarities of cyberspace and the challenges of cyber crises make it necessary to engage in a proactive cyber crisis management. Cyberspace is becoming increasingly contested in which absolute defence and attribution are extremely difficult, if not impossible. Comprehensive cyber crisis management must thus include proactive strategies to prevent crises before they arise. All three conclusions must be considered when aiming at engaging in international cyber crisis management. Therefore, they form the basis of three salient discourses on managing crisis in cyberspace: securitisation, convergence and deterrence. The next chapter will introduce the three discourses and place them in the causal mechanism that has been established in Chapter 1.

Chapter 3: Discourses of Cyber Crisis Management

As we can recall, discourses are the reflexive articulation of cognitive and normative ideas between actors. Discourses in relation to the ideas matrix can happen on the philosophical, programmatic or the policy level. Discourses are shown to cause institutional change but also be responsible for incomplete institutional reform. In the context of European integration, discourses are the driving force of the proposed causal mechanism, which is why it is important to examine salient discourses in the policy field one tries to apply this mechanism. Based on the conceptualisation of cyberspace and cyber crisis I will now introduce the discourses on *securitisation, convergence* and *deterrence*. I will furthermore introduce a hierarchy of the discourses, in relation to their placement in the matrix of ideas. Securitisation sits at the top of this hierarchy, as it is a discourse on the philosophical level. Convergence and deterrence are

then derived from this underlying discourse. They are to be placed at the programmatic level as they contain ideas that define specific policy problems and provide frameworks for dealing with them. What follows is that a causal mechanism, specific to the field of cyber crisis management can be introduced, based on the discourses of securitisation, convergence and deterrence.

A Discourse of Securitisation

The discourse on securitisation of cyberspace is based on premise that security is socially constructed. Approaches of defining security evolved since the end of the Cold War. This trend is related inter alia to the growing importance of non-state actors, a globalisation of threats and dangers and technological advancements. The Human Development Report issued in 1994 by the United Nations Development Programme has largely contributed to introducing the concept of human security. The aim was to consolidate an understanding of security that goes beyond the military dimension, which is highly related to the nation-state and territory (Paris, 2001). This paradigm shift in defining security has pathed the way for introducing the human dimension to security and given importance to the human perception of what security means. Subjective security has gained more prominence and has led to a conceptualisation that includes material factors, as well as human perception, and established a relation between them. Security in this context is then a reflexive interaction between subjective perceptions and material structures. Ideas about how things are, shape the way actors interact with the given material structures. Actors may choose to alter material structures if they believe that it increases their security. This process is a dynamic one, that includes a rearticulation of what security is and how to achieve it. In that way, security is socially constructed and perpetually redefined, dependent on human perception of material structures. This does not exclude a military dimension, the nation-state or territory, but establishes a correlation between the physical, "objective" form of security and the perceived, "subjective" dimension (Hyde-Price, 2001).

By constituting security as socially constructed, it is possible that a policy area, that had previously not been part of a security agenda, can become securitised and thus gain political relevance. Cyberspace in that manner becomes part of the security agenda, as it is perceived to belong there. For this to happen, the idea must be consolidated, that cyberspace is a terrain that is firstly vulnerable to threats and risks, and secondly that it is necessary and worth to be protected. In relation to the matrix of ideas, a securitisation of cyberspace contains cognitive and normative ideas. The cognitive part of this discourse is heavily linked to the

conceptualisation of cyberspace and ongoing societal dynamics. As discussed earlier, the particularities of cyberspace render it to be of a malleable and borderless nature, in which there is a proliferation of potential adversaries, to which it is very difficult to attribute malicious behaviour. This means that offensive strategies in cyberspace are favoured and there is no absolute defence against cyberattacks. Cyberspace thus carries a variety of systematic and humanmade risks and threats, which becomes increasingly contested. Additionally, societal trends as digitalisation render malicious behaviour in cyberspace to have a greater impact. Societies have become increasingly dependent on ICTs, a trend that can be observed to have accelerated in the wake of the COVID-19 pandemic (Carrapico & Farrand, 2020). Parallel to an increased vulnerability of societies, offensive capabilities are continuously being developed, which must lead to an expectation that the number of cyber incidents will rise and their impact will be greater (van der Meer, 2016). As societies become more vulnerable and offensive cyber capabilities are proliferated, cyber crisis in this context becomes a tangible threat. The conceptualisation of a cyber crisis, within the securitisation discourse is essential, as it makes way for programmatic and policy ideas to be derived from it. As the possibility of a cyber crisis is established, the need for cyber crisis management is introduced and ideas of how to manage them are articulated. The cognitive side of the securitisation discourse thus relates the systemic risks of cyberspace, with societal trends and establishes cyberspace as a contested domain in which there is potential for cyber crisis.

The normative level of securitisation can be explained by the linking of cyberspace to other referent objects as the ‘state’, ‘society’ or ‘economy’. Within the discourse, cyberspace is causally related to these referent objects, as it is framed to be a fundamental part of them. Securing political systems, societies or economies thus becomes analogous to protecting cyberspace. A need to secure cyberspace is introduced, as the consequence of not doing it would mean insecurity for the referent objects. This feeds into underlying normative constellations, which in the context of states carry the idea that protecting its citizen is not only good, but also necessary. (Hansen & Nissenbaum, 2009). Cyber crisis in this context, as an escalation of cyber incidents has the potential to cause great harm to the referent objects. It can even pose an existential threat, which means that managing cyber crisis is deemed to be of utmost importance.

The securitisation discourse thus carries cognitive and normative ideas at the philosophical level, which can completely alter an actor’s worldview and normative constellation, as cyberspace becomes part of the security agenda. Cyberspace is introduced as

a terrain that is vulnerable due to systemic risks and societal developments, and that needs to be protected as not doing so would impact referent objects. The conceptualisation of cyber crisis is a fundamental part of the securitisation process, as its possible occurrence imposes the greatest imaginable impact on the referent objects of the state, economy and society and introduces the need for managing cyber crisis. Securitisation is thus a discourse of cognitive and normative ideas at the philosophical level, which includes societal trends (cyberspace becomes increasingly contested, vulnerabilities arise as societies become more dependent on ICTs) and conceptualises cyber crisis and their impacts (impact of large-scale cyber incidents can have devastating impacts on economies, societies and fundamental values).

A Discourse of Convergence

The second discourse to be examined contains the programmatic idea of cyber crisis management through convergence. Convergence has since its introduction become an indication of actorness in the transboundary crisis management literature (Backman & Rhinard, 2018; Boeke, 2018; Boin, Rhinard, & Ekengren, 2014; Carrapico & Barrinha, 2017). Based on the conceptualisation of a potential crisis that is rooted in the underlying philosophical ideas or securitisation discourse, convergence is an approach to manage crisis in cyberspace. The cognitive idea is that cyber crisis, as a transboundary phenomenon poses a set of political-administrative challenges to its management. Convergence is introduced as a way to deal with these challenges and conduct comprehensive cyber crisis management. Convergence in this sense is defined to have two aspects: coherence in institutional structures and coherence in perception. Firstly, convergence comes in the form of institutional coordination. Operational and political processes in crisis management must be harmonised, to ensure the smooth functioning. In the context of a transboundary crisis, the reduction of friction between all the affected policy areas and actors is key. When institutional structures are not harmonised to a certain extent, the management of an incurring crisis can be inefficient or incomplete and render the actor incapable of sufficiently minimising harm. Secondly coherence must include a shared understanding of the security environment. If the multiple actors being involved in the management of a transboundary crisis do not share the same sense of what is going on and how to act in a given situation, timely and effective crisis management is rendered impossible (Carrapico & Barrinha, 2017).

As convergence becomes a measurement for effective transboundary crisis management, it has been applied to test the capabilities of crisis management actors. In relation to the conceptualisation of cyber crisis, coherence is measured in the areas of the political-

administrative challenges of transboundary crisis management: detection, sense-making, decision-making, coordination, meaning-making and accountability. It is believed to be beneficial to introduce hierarchical structures to these areas, in order to cope with the transboundary nature of crisis. A centralised approach for managing transboundary crisis has the advantage of preventing conflicting understandings of a crisis situation and introduce standardised operational and political procedures, that increase an actors responsiveness (Backman & Rhinard, 2018).

The discourse on convergence is thus programmatic one. It takes the underlying philosophy that cyber crisis potentially cause a great deal of damage in an increasingly contested domain. It then goes on to define the challenge of timely and effective management and proposes to address it by introducing convergence of institutional structures and security perceptions. As the cognitive idea of introducing convergence to manage cyber crisis constitutes mainly a change in administrative structures, one might argute it has low potential of conflicting with normative constellations. Convergence does not challenge the underlying normative philosophy is that securing cyberspace is good and necessary and may therefore be considered legitimate. However, in the context of the European Union and its Member States, cognitive ideas of convergence that are viewed as functional and legitimate on a supranational level, might be considered dysfunctional or illegitimate on a national level. This can arise as national discourses perceive convergence not to be capable to manage crisis in cyberspace or, that the existing institutional setup is insufficiently elaborated. Furthermore, the idea of convergence may not conflict with supranational normative constellations, but very well with normative constellations on the national level. Convergence, even if it may be perceived as the best way of managing cyber crisis can conflict with norms of national sovereignty. This may lead to incomplete institutional change, which again causes further integration.

In summary, convergence is a discourse at programmatic level that can be derived from securitisation. It defines the main challenges of supranational cyber crisis management, linked to the particularities of cyberspace (responding in a timely and coordinated manner, as cyber crisis can spread quickly across borders) and introduces a possible solution (convergence of supranational structures and perceptions of the security environment).

A Discourse of Deterrence

The final discourse contains the idea of cyber crisis management through deterrence. The rationale behind it is rooted in the peculiarities of space. As it has been conceptualised before,

cyberspace makes it impossible to follow a strategy of absolute defence, and possible for adversaries to potentially stay undetected for ever. This means that actors engaging in offensive malicious behaviour can do so in the hopes of eventually overcoming the defensive capacities of a network and do so covertly. This prospect makes it very attractive for an actor to engage in such behaviour, as cyberspace seems to favour offensive strategies over defensive ones. What follows is the need to mitigate the unfavourable defensive position.

A way to do that is by engaging in a strategy of deterrence to dissuade adversaries from engaging in malicious behaviour in the first place. Deterrence is a strategy that originated in the wake of the Cold War, in relation to the proliferation of nuclear weapons. There are two ways in which deterrence can be practiced: deterrence by denial and deterrence by punishment. Deterrence by denial is based on the signalling of great defensive capabilities, that makes the offensive efforts of adversaries a hopeless endeavour. An adversary must be convinced, that any form of attack is rendered ineffective due to the impenetrable defences of an actor (Krepinevich, 2019). Deterrence by punishment on the other hand is based on the signalling, that any malicious act will cause retribution, that by far outmatches any possible gain from engaging in them in the first place. Adversaries are thus dissuaded from attacking, because the potential losses they experience are believed to be greater than the possible benefits. Legitimacy of threat is gained, if an actor has previously engaged in retribution, which serves as a precedent for potential adversaries (Lancelot, 2020).

Joseph Nye is one of the most prominent advocates for the applicability of deterrence strategies to cyberspace. In his article on Cyber Power, he states that “Cyber war can be managed through inter-state deterrence, and offensive capabilities plus resilience if deterrence fails.” (Nye, 2010, p. 16). By building up great offensive cyber capabilities and communicating openly about them, is said to deter adversaries from engaging in cyberattacks. This view is however strongly contested by the academic literature. Scholars, who have taken the peculiarities of cyberspace into consideration, argue that deterrence is a declining concept, which is inapplicable to cyberspace. The reason is that cyberspace does not allow for either effective deterrence by denial or deterrence by punishment. Deterrence by denial in cyberspace is considered to be impractical, as the particularities of cyberspace make defending very hard. Cyberspace is a borderless domain, of which the structure is constantly changing, and new technologies emerge continuously. As previously discussed, absolute defensive strategies are considered to be impossible. This delegitimises the signalling an impenetrable defence and renders deterrence by denial impracticable. Deterrence by punishment is equally difficult, as

the problem of attribution infringes the legitimacy of threatening grave retribution. Cyberspace allows actors to be anonymous and stay undetected whilst engaging in malicious activities. Attribution is very costly and time consuming and may never produce absolute certainty about the identity of an actor. Signalling the engagement in grave retribution loses its legitimacy, as firstly, adversaries may never be identified and secondly, a residual uncertainty may always remain. Would a state respond cyberattack by crossing the threshold of kinetic war, with only a 99% certainty about who attacked them? (Harknett & Smeets, 2020).

Deterrence, even though it being a highly contested concept is still substantial part of cybersecurity strategies across the world (Manantan, 2021). In the context of cyber crisis management, it is framed to prevent cyber incidents from happening, or constitute an effective response, which in turn sets a deterring precedent. The discourse on deterrence is one that is way more heterogeneous than the discourse on convergence. There are two reasons for that. Firstly, there are conflicting conceptual ideas of the functionality of deterrence in managing crisis in cyberspace. Deterrence my either be perceived as a valuable tool in complementing defensive efforts of cyber crisis management, or to be a strategy inapplicable to cyberspace. Its functionality is thus heavily contested from the outset. Secondly, deterrence includes the use of some form of offensive capability, which may conflict with existing normative constellations at the supranational level. Deterrence, even if perceived to be functionally the best approach of managing crisis in cyberspace could be deemed illegitimate, as it would conflict with the norm of peaceful settlement of conflicts, that is deeply enshrined in the EU. Furthermore, deterrence on a supranational level may again conflict with national norms of national sovereignty, as Member States are reluctant to converge more powers to the EU in the field of the CFSP. As the concept of deterrence is heavily contested it is expected that institutional change establishing ideas of deterrence are incomplete and will lead to further institutional change.

In summary the programmatic discourse of deterrence defines a main challenge of supranationally managing crisis in cyberspace, linked to cyberspace itself (reactive strategies of managing cyber crisis are incomplete as cyberspace favours offensive behaviour) and offers a solution (introducing the proactive strategy of deterrence to prevent cyber crisis). What follows now is that we can introduce a causal mechanism for European integration in the field of cyber crisis management. Contrary to the existing literature which puts a crisis at the beginning of a causal chain for integration, the discursive approach allows integration to happen without the necessity of an actual crisis.

The causal mechanism on European integration in the field of cyber crisis management looks as follows. A securitisation discourse containing the conceptualisation of a cyber crisis starts the integration process in the field of cyber crisis management. A need to manage cyber crisis due to its devastating impact on referent objects is generated. The discourses of convergence and deterrence then introduced problems of managing crisis in cyberspace and offered solutions. Conflicting supranational and national discourses in regard to national sovereignty and conflicting cognitive and normative ideas concerning offensive capabilities lead to an incomplete institutional reform. Further integration is then triggered again, if the incomplete institutional reforms are perceived as such in relation to their functionality or legitimacy and follows a path of institutional layering.

Conclusion Part I

Part I has now established three things. One, discourses have power in explaining institutional change. Discourses can change institutional structures as they change the cognitive or normative ideas of actors at the philosophical, programmatic or policy level. Instructions change as worldviews or normative constellations of actors change, new problems and means of addressing them are defined or if the perception of the functionality or legitimacy of existing ideas change. Institutional reform may however be incomplete due to conflicting national and supranational discourses or incompatibilities between cognitive and normative ideas.

Two, the particularities of cyberspace and cyber crises shape the discourses of cyber crisis management. Cyberspace is malleable and borderless terrain, that empowers the individual and makes attribution very costly, time consuming or impossible. Increasing digitalisation and a continuous evolvement of potentially harmful capabilities render cyberspace to be an increasingly contested domain of strategic interaction. Cyber crisis in this context is conceptualised to have particular political-administrative challenges, that distinguishes it from conventional crisis. What follows is that cyberspace renders societies increasingly vulnerable to a growing dependence on ICTs, cyber crisis is a transboundary phenomenon that is best managed at an international level and engaging in proactive strategies is necessary to conduct comprehensive cyber crisis management.

Three, the discourses of securitisation, convergence and deterrence are based on the peculiarities of cyberspace constitute incremental parts of the causal mechanism in the integration process in the field of managing crisis in cyberspace. The securitisation discourse introduces the need for cyber crisis management. The discourses on convergence and

deterrence then define problems of cyber crisis management and propose possible solutions. The integration process is then advanced as incomplete institutional reforms from conflicting discourses cause the introduction of new institutional change. Part II will now examine EU policies as steps of integration in the light of the established causal mechanism of European integration in the field of cyber crisis management and give an account on the future of the European CCMR.

Part II - European Integration in the Field of Cyber Crisis Management

The second part of this thesis will now trace the integration process in the field of cyber crisis management in the EU. The cornerstone of the analysis will be the application of the causal mechanism established in Part I. It will be applied to the case study by applying 'efficient process tracing'. Based on conventional forms of process tracing, an outcome is linked to causal mechanisms within boundaries constructed by the researcher (Lauth et al., 2016). Efficient process tracing is then an approach tailored towards European integration. Process tracing in the form of a single case congruence study, allows for capture the specific nature of the EU as a phenomenon sui generis. What is required is an ex-ante specification of the causal mechanism and then testing the expectations derived from it match the explanatory factors of European integration. By defining the causal mechanism ex-ante, it is possible to avert the danger of engaging in storytelling. Instead of simply describing the evolution within a given policy field, efficient process tracing allows for diagramming a causal chain that depicts the integration process in a convincing manner. Another important aspect of efficient process tracing is defining relevant actors. In the context of this thesis and its approach I choose to differentiate between supranational discourses (EU institutions, and agencies) and national discourses (of Member States). They are however not mutually exclusive, can overlap in many ways and also be substantial in influencing and shaping each other (Schimmelfennig, 2015).

The causal mechanism will then be applied to EU legislative and non-legislative acts concerned with cyber crisis management. The main sources for examining the causal mechanism established will be the Cyber Security Strategy of the EU (CSSEU) of 2013, the Directive Concerning Measures for a High Common Level of Security of Network and Information systems across the Union or 'NIS Directive' of 2016, the Commission Recommendation on Coordinated Response to Large-scale Cybersecurity Incidents and Crises, or 'Blueprint' of 2017 and the Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities, or 'Cyber Diplomacy Toolbox'. The Cyber Security

Strategy of 2013 is chosen as it first established the cyber domain as an own policy field. It furthermore includes the guiding ideas how cyberspace shall be perceived and interacted with. It is thus one of the key documents of the securitisation discourse. The NIS Directive will be examined, as it has its roots in the CCEU and introduced a crisis cooperation mechanism at the technical level. Furthermore, it is perceived as the main catalyst for the Blueprint. The Blueprint is chosen as it is the most important step of integration in cyber crisis management to date. It sets up a framework of how to respond to incurring cyber crisis, that includes all the different actors, mechanisms, and tools. It is thus the prime example of the discourse on convergence. Lastly, I choose the Cyber Diplomacy Toolbox to examine the discourse on deterrence. The toolbox established a framework of coordinated sanctions, that are meant to respond to cyberattacks, but also contribute to crisis management through preventing future incidents through the logic of deterrence by punishment. Additionally, to these three documents, information from five semi-structured interviews with EU policymakers, civil servants and cybersecurity experts will be utilised to trace the causal mechanism.

The causal mechanism will be traced by examining the EU documents by applying the following operationalisation of discourses. Securitisation is a discourse at the philosophical level, which includes societal trends (cyberspace becomes increasingly contested, vulnerabilities arise as societies become more dependent on ICTs) and conceptualises cyber crisis and their impacts (impact of large-scale cyber incidents can have devastating impacts on economies, societies and fundamental values). Convergence is then a discourse at programmatic level that can be derived from securitisation. It defines the main challenges of supranational cyber crisis management, linked to the particularities of cyberspace (responding in a timely and coordinated manner, as cyber crisis can spread quickly across borders) and introduces a possible solution (convergence of supranational structures and perceptions of the security environment). In the same way, the programmatic discourse of deterrence defines a main challenge of supranationally managing crisis in cyberspace, linked to cyberspace itself (reactive strategies of managing cyber crisis are incomplete as cyberspace favours offensive behaviour) and offers a solution (introducing the proactive strategy of deterrence to prevent cyber crisis). By examining the different steps of European integration in regard to the discourses it is possible to test for the proposed causal mechanism for European integration. Chapter 5 will then reflect on the future of EU cyber crisis management and the EU's capability of managing crisis in cyberspace.

Chapter 4 will now go on trace the causal mechanisms introduced in Part I in the European integration process of cyber crisis management. It will do so by firstly outlining the existing components of the current Cyber Crisis management regime of the EU and then go on to examine the Cybersecurity Strategy of 2013, the NIS Directive of 2016, the Blueprint of 2017 and the Cyber Diplomacy Toolbox of 2017. These documents will be examined in the light of the discourses of securitisation, convergence and deterrence.

Chapter 4: The Evolution of the EU Cyber Crisis Management Regime

Tracing European integration is a process that links an outcome with causal mechanisms. Therefore, it makes sense to take stock of the current EU cyber security eco system in relation to cyber crisis management. First however, it is important to give a context of the EU's CCMR. First, it is important to stress that the EU does not exist in a vacuum. For one, the behaviour of the EU is not only guided by its own institutional structures, but also by international law. The European Union commits itself to strictly observe international and develop international law, which forms part of its institutional structures (Art. 3(5), TEU). In the context of the cyber domain, the 2015 report of the United Nations Group of Governmental Experts (UN GGE) on the Developments in the Field of Information and Telecommunications in the Context of International Security, established a four-pillar system. It contains the applicability of international law, especially the UN Charter, Art 2(4), Confidence building measures (CBMs), international cooperation and capacity building, and norms, rules and principles for responsible state behaviour in cyber space. This four pillar system forms the guiding principles of states' behaviour in cyberspace to which the EU adheres (Gursch-Adam, 2022). A second way in which the EU is influenced by the international context is through its Member States' the obligations in other international organisations. In the context of cyber domain, the main actors are the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organization (NATO). The EU's Member States make up 27 of the 57 participating states in the OSCE, 21 of them are in NATO, with accession protocols ready to be ratified in Sweden and Finland, and all of the EU members are part of the UN (Globe, 2020). Discourses within these organisations may thus influence institutional structures of the EU. For the sake of this thesis however, they will not be explicitly examined, as they are assumed to either influence discourses of supranational or national actors.

Secondly, it is important to define the EU's competences in managing crisis in cyberspace. In general, the EU's competences for cyber crisis management can be found within the provision of the EU Treaties on the Area of Freedom Security and Justice, the CSDP, and

with the introduction of cyber diplomacy, the CFSP. As in other domains of crisis management, Member States have the primary obligation of managing large-scale cybersecurity incidents or cyber crisis that are affecting them. The EU has principally a facilitating role of resource pooling and information sharing and has established a network of actors, crisis management mechanisms, and coordinative structures to assist in cyber crisis management. However, in the case of a cyber crisis, Member States can trigger either the Solidarity Clause (Art. 222, TFEU) or the Mutual Defence Clause (Art. 42(7), TEU), depending on the severity of the incident.

Lastly, it is important to provide the commonly applied definition of a cyber crisis within the EU. The EU applies the following definition of a cyber crisis:

> "A cybersecurity incident may be considered a crisis at Union level when the disruption caused by the incident is too extensive for a concerned Member State to handle on its own or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level." (European Commission, 2017, p. 1).

This definition is highly important as it frames the approach of the EU to manage crisis in cyberspace and points to the fact, that no cybersecurity incident in the EU has thus far qualified as a cyber crisis.

The EU's Cyber Crisis Management Regime

The existing cyber crisis management regime of the EU consist of various actors, crisis management mechanisms and coordinating structures across multiple cyber communities. The following is an attempt to provide an extensive, yet not exhaustive account of the fragmented system that is the EU's CCR.

The multiple *actors* within the cybersecurity ecosystem can be categorised into four cyber communities. They all comprise actors on the EU and Member State level. First there is the community of civil cybersecurity, or resilience. This community comprises the European Union Agency for Cybersecurity (ENISA), the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU), the National Computer Security Incident Response Teams (CSIRTs), the Cyber Crisis Liaison Organisation Network (CyCLONe), the Cooperation Group on Security of Network and Information Systems and the Security Operation Centres (SOC). The second community is law enforcement incorporates the European Cybercrime Centre ('EC3') and its Joint Cyber Crime Taskforce ('J-CAT'), which

was established within Europol. The third community is the one of cyber diplomacy and includes the European External Action Service (EEAS) with the intelligence coordination networks of the EU Intelligence Analysis Centre (INTCEN) and EU Military Staff (EUMS) Intelligence Directorate (EUMS INT), and the Horizontal Working Party on Cyber Issues. The fourth cyber community is concerned with cyber defence and includes Permanent Structured Cooperation (PESCO) and the European Defence Agency (EDA) (European Commission, 2021b).

The *cooperation mechanisms* of cyber crisis management are carried out at either a technical, operational or strategic/political level. At the technical level, the EU directive concerning measures for a high common level of security of network and information systems across the Union, or NIS Directive has established the National Computer Security Incident Response Teams (CSIRTs). The CSIRTs are composed of national experts that ensure effective cooperation and timely response to cyber incidents. Coordination at the strategic/political level is located in the Horizontal Working Party on Cyber Issues within the Council. In the event of a cyber crisis its primary task is to coordinate a diplomatic response in the context of the Cyber Diplomacy Toolbox. At the operational level, coordination is conducted in the Cyber Crisis Liaison Organisation Network (CyCLONe). This was formally established through the Commission's proposal for a NIS 2 directive but has its roots in the introduction of the 'Blueprint' (Interview 5).

Furthermore, there are different *crisis management mechanisms* for responding to incurring cyber crisis. There are three mechanisms: the rapid alert system ARGUS of the Commission, the Integrated Political Crisis Response (IPCR) of the Council and the Crisis Response Mechanism (CRM) of the EEAS. All these mechanisms have distinct procedures in responding to incurring crisis. Currently these mechanisms are not harmonised. There is however an initiative to introduce standard procedures of interaction between the mechanisms, which can be related to a discourse on their incompleteness and dysfunctionality in the face of an incurring crisis.

To add to this already complex environment policies related to cyber crisis management can be grouped into the four steps of the crisis management cycle: prevention/mitigation, preparedness, response and recovery. Different cyber communities engage in different or multiple areas of the crisis management cycle. All of the communities must engage sufficiently

in policies within the crisis management cycle, as their capabilities are not connected across communities (Trimintzios et al., 2015).

I will now go on to examine four EU documents in the light of integration in the field of cyber crisis management: The Cybersecurity Strategy of 2013, the NIS directive of 2016, the 'Blueprint' of 2017 and the Cyber Diplomacy Toolbox of 2017. I will proceed by introducing the discourses that lead to their establishment, outline the content of the policies, examine the content in regard to the discourses of securitisation, convergence and deterrence, and show how they led to further integration due to conflicting discourses on their functionality or legitimacy. I will proceed chronologically.

The Cybersecurity Strategy 2013

The *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (CSSEU) was published in 2013 as a joint effort of the European Commission and the High Representative. It was introduced in a time that saw the change of the general cybersecurity discourse from a Computer-Centric and IT-Centric, to an Information-Centric era (Eling et al., 2021). As information became more valuable, a discourse emerged on the necessity of its protection. With the turn of the century, the European Commission launched its Communication on Network and Information Security: Proposal for a European Policy Approach (European Commission, 2001). In this communication, the importance of protecting information networks was stressed and cyberspace was linked to questions of security for the first time. Cyberspace has since then been increasingly framed as a contested domain that is in need of protection by the EU (Christou, 2019). The discourse on securitisation was however driven mainly by protecting the European economy and building public-private partnerships. Cyberspace was perceived to be dangerous to the smooth sailing of the growing European economy and must therefore be protected. With the publication of the Internal Security Strategy (European Commission, 2010b) in relation to the introduced Digital Agenda for Europe (European Commission, 2010a), the discourse became solidified and EU cybersecurity policy became 'formalised'. The economy was still constituted the main necessity for cybersecurity within the EU. However, the dangers created by cyberspace to political systems was stressed in relation to incidents as the attacks on Estonian network and information systems and introduced a focus on cybersecurity, rather than solely on cybercrime.

This continuous evolution of the securitisation discourse led to, the introduction of the CSSEU in 2013, based on a proposal of the Commissions' Directorate-General for

Communications Networks, Content and Technology (DG CONNECT). Its introduction must not be perceived as the response to rising cyber incidents, but as a culmination of the securitisation discourse, which also has an international dimension. In the preceding years of the CSSEU, no unexpected increase in cyberattacks could be detected, nor was there a major incident that could be understood as a shock that caused European integration. The cause for the CSSEU was rather the evolving securitisation discourse within the EU and an international discourse, perpetuated by the introduction of national cybersecurity strategies around the globe, that is explicitly mentioned in the CSSEU (Interview 2).

The strategy was introduced to set out an EU vision of cyberspace, define roles and responsibilities, and outline required action for 'strongly protecting and promoting citizens' rights, to make the EU's online environment the safest in the world.' (European Commission & High Representative, 2013, p. 3). It set outs strategic priorities of cyber resilience, reducing cybercrime, developing a cyber defence policy within the CSDP, industrial and technological cybersecurity resources, and uphold EU norms in a coherent international cyberspace.

Throughout the elaboration of these goals and the respective planned action, the securitisation discourse can be found along each step of the way. First, the CSSEU frames cyberspace as a contested domain. While referring to the benefits as the empowerment of the individual, that was to be observed during the Arab Spring, it points to the great challenges for EU citizens, the European economy and the EU's norms and everyday life. The continuous reference to the fundamental values of fundamental rights, democracy and the rule of law, which must be upheld in cyberspace points to the fact that the securitisation discourse not only has a cognitive, but also a strong normative component. Second, the CSSEU refers to the increased vulnerabilities due to an increasing dependence of ICTs. It states that "The growing dependency on information and communications technologies in all domains of human life has led to vulnerabilities which need to be properly defined, thoroughly analysed, remedied or reduced" (Ibid., p. 4). Third, it points to the unique nature of cyberspace, in particular that "Cyber incidents do not stop at borders in the interconnected digital economy and society." (Ibid., p. 17). This part introduces the potentially devastating impact of a large-scale cybersecurity incident, or cyber crisis. Finally, the CSSEU introduces the EU as an actor, that it at least in part responsible for managing cyberspace and its arising threats. It says that cyberspace must be protected "[…] due to the potential or actual borderless nature of the risks, an effective national response would often require EU-level involvement" (Ibid., p.17).

The CSSEU consolidated an already existing discourse on the securitisation of cyberspace within the EU and showed both a cognitive, but also a strong normative component. It constituted cyberspace as an increasingly contested domain, framed a rise in vulnerabilities, pointed to the borderless nature of cyberspace, conceptualised the potential impact of cyber crises and constituted itself as a cyber security actor. It additionally introduced the cyber domain as a distinct field of EU policy and was the first EU document to address the necessity of building EU cyber defence capacities, which would later on materialise in the form of the EU Cyber Defence Policy Framework (Council of the European Union, 2014). The most important component for further European integration of the CSSEU, was directive on network and information security (NIS), that was proposed alongside it. It introduced the discourse on convergence, set out future agenda on harmonising structures, and will be discussed next. Overall, the CSSEU must thus be regarded as the consolidation of an evolving securitisation discourse, and as a catalyst for European integration in the cyber domain, and specifically in cyber crisis management.

The NIS Directive 2016

The *Directive Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*, or 'NIS Directive' was published on 6 July 2016. It was the result of continuous negotiations taking place since it was proposed in the CSSEU in 2013. The reason for its contested initiation can be explained through its content, and confliction national and supranational discourses.

The NIS Directive was the first EU legislation on cybersecurity. Its aim was to introduce EU wide standards of network and information systems security. It does so by a) introducing an obligation for Member states to adopt a national strategy to secure network and information systems, b) establish a Cooperation Group for information sharing, cooperation and building confidence, c) create a network of computer security incident response teams (CSIRTs network) for timely and effective operational cooperation, d) requires the securing and reporting of essential service providers and e) obliges Member States to establish single points of contact, national competent authorities and CSIRTs.

The NIS is the clear policy materialisation of a programmatic convergence discourse, that originated in the CSSEU. It refers to the securitisation discourse by stating that "[t]he magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems." and that "[o]wing to that

transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole." (European Union, 2016, p. 1). It then goes on to define the problem that "Member States have very different levels of preparedness, which has led to fragmented approaches across the Union." (Ibid., p. 2), and introduce the solution in form of introducing obligation for the convergence of minimum NIS security standards. Convergence in this sense includes a coordination of operational structures, as well as information sharing for establishing a common understanding of the threat environment.

The NIS Directive was aimed to address the great divergences in cybersecurity and cyber crisis management capabilities. The divergence can be explained by a lack of national discourses on the necessity of introducing coherent and comprehensive cybersecurity policies. The fewest Member States had established a cybersecurity strategy or national CSIRTs. The directive thus tried to mitigate these divergences, as large-scale cyber incidents, or cyber crisis were perceived to have a transnational or European wide effect. The process of introducing the NIS directive lasted three years since its proposal within the CSSEU and was one of tough negotiations. It is a prime example of conflicting discourses on the supranational and the national level. While the European discourse clearly framed the necessity for introducing new obligations in establishing minimum standards, national sovereignty discourses opposed these ideas. especially the obligation of reporting cyber incidents that affected critical entities and sharing information on cybersecurity standards was perceived to be a violation of national sovereignty. Member States were reluctant to unveil the bad state of their national cybersecurity infrastructures which lead to an extensive process of negotiation. It must be stressed however, that there were also national discourses that supported the supranational ambitions, mostly coming from states with more elaborated cybersecurity policies. As the years passed, the securitisation discourse spread across more Member States, and was increasingly linked to the protection of the citizens, political systems and in that matter, of national sovereignty. The national and supranational discourses finally converged, as introducing supranational standards came to be perceived as a requirement for sovereignty and national security (Interview 1).

The NIS Directive must be considered one of the most important steps of European integration in the cyber domain and in cyber crisis management. As a directive, it constitutes a step of 'hard' integration as it introduced binding obligations to the Member States. It was established through the programmatic discourse of convergence established in the CSSEU and

fostered institutional change through introducing convergence policies. Its introduction was the result of years long negotiations that was postponed through conflicting national and supranational discourses. The cognitive ideas of introducing convergence in cybersecurity standards clashed with national normative constellations, especially 'national sovereignty'. After being introduced in 2016 its set in motion a process of further integration based on the discourse on convergence. Regarding the existing cyber crisis management regime, the NIS introduced the technical component of European coordination in responding to cyber crisis. It is therefore widely considered to be the most important steppingstone to the Commission's recommendation introducing a framework for responding to large-scale cybersecurity incidents in a coordinated manner: the 'Blueprint'

The 'Blueprint' 2017

The main step of European integration in the field of managing crisis in cyberspace was the *Commission Recommendation on Coordinated Response to Large-scale Cybersecurity Incidents and Crises*, or 'Blueprint' of 2017 (European Commission, 2017). It was introduced on the initiative of the Commission and outlines the modes of cooperation and objectives of the EU institutions and Member States in responding to large-scale cybersecurity incidents and crises. The introduction of the Blueprint is central to this thesis, as it supports its main claim that discourses hold great explanatory power for European integration. The Blueprint grew out of the supranational programmatic discourse on convergence as can be derived from analysing its content. The NIS directive, as a forerunner of this discourse, was constitutive of the Blueprint, as it introduced the CSIRTs Network as a technical cooperation mechanism, as an addition to the Council Horizontal Working Party on Cyber Issues as a political and strategic mechanism. In the same way as the NIS directive, a supranational discourse called for the necessity of a framework for coordinated cyber crisis management. The most important part to this thesis is, that the framework was set up with the conceptualisation of the tremendous impact of potential cyber crisis in mind. The establishment of the Blueprint is the core piece of the proposed discursive causal mechanism of European integration, as it shows that the mere conceptualisation of a cyber crisis has led to its establishment. This argument is supported not only by regarding the discursive developments before the introduction of the blueprint, but also through looking at Article (2) of the Blueprint, which prominently features the previously introduced definition of a cyber crisis in the context of the EU (European Commission, 2017, p. 36). The introduction of the Blueprint is thus the result of an evolving securitisation discourse containing the conceptualisation of a cyber crisis, that lead to the programmatic idea

of convergence which culminated in its most elaborate iteration in the form of the Blueprint. I will now introduce the content of the Blueprint and trace its convergence discourse.

The core objectives of the Blueprint are to enable an effective response, a shared situational awareness and common key messages in crisis communication. It then defines the actors, introduces the objectives for situational awareness, gives possible responses and presents challenges of public communication for the already existing crisis management coordination mechanism on the operational level (CSIRTs Network) and the political/strategic level (Council Horizontal Working Party on Cyber Issues). It furthermore does the same for an operational cooperation mechanism, that had not been established to date. By hypothesising how a potential operational capability could take shape, the Blueprint established the , but will evolve as the result of the Blueprint. More on that later. The Blueprint goes on to clarify the processes in response to an incurring cyber crisis within the existing crisis management mechanisms of the IPCR, ARGUS and the EEAS CRM (European Commission, 2017). What this gives us is the most elaborate framework of how cyber crisis management should be conducted on the EU level. It furthermore is the most comprehensive consolidation of the discourse on convergence, which I will examine now.

Tracing the discourse on convergence in the Blueprint is not a difficult endeavour, as its whole purpose is to introduce a framework for convergence through coordinative structures and shared situational awareness. I will therefore only choose representative examples for its link to the securitisation discourse, its problem definition and its proposed solution. The Blueprint refers to the securitisation discourse by stating that "[…] the dependence on information and communication technologies have become fundamental […]" and that "[c]ybersecurity incidents can trigger a broader crisis, impacting sectors of activity beyond network and information systems and communication networks […]" (European Commission, 2017, p. 36). It then introduces the problem of timely and large-scale response to a cyber crisis through defining that "[c]ybersecurity incidents are unpredictable, often occur and evolve within very short periods of time and therefore affected entities and those with responsibilities as regards responding to and mitigating the effects of the incident must coordinate their response quickly." (Ibid., p. 36). In the spirit of the convergence discourse, the Blueprint provides a solution for a timely and comprehensive cyber crisis management claiming that "[a]n effective response to large-scale cybersecurity incidents and crises at the EU level requires swift and effective cooperation amongst all relevant stakeholders and relies on the preparedness and capabilities of individual Member States as well as coordinated joint action

supported by Union capabilities" (Ibid., p. 36). The Blueprint is the most representative example of how the discourse on convergence can take shape. It aims throughout at converging structures and perceptions to manage the vulnerabilities created by the increasing dependence on ICTs. The EU's cyber crisis management has in the Blueprint attained a very comprehensive framework for dealing with the transboundary management of potential cyber crisis.

The Blueprint is however not only the policy materialisation of the discourse on convergence, but also emblematic on how incomplete institutional structures cause new discourses that in turn lead to further integration. The Blueprint has established the operational level of cyber crisis management and proposed an information sharing platform, which has however never been consolidated. Within the Cooperation Group on Security of Network and Information Systems, a particular Member State started a discourse on the functionality of this platform and the operational level in general. The reason for the discourse was, that the Member State perceived the operational level to be dysfunctional. What came out of this discourse was a joint exercise of cyber crisis management called Blue OLEx, first carried out in Paris in 2019. The exercise produces an after-action report that contained several lessons learned, as the necessity for contact lists of crisis management actors, secure means of communication and communication guidelines in the case of a crisis. The joint exercise and its after action report led to the launch of the Cyber Crisis Liaison Organisation Network (CyCLONe), an informal coordination network between cyber crisis management agencies of the EU Member States. It was launched during yet another Blue OLEx exercise in 2020 within the context of the Commission's proposal for a NIS 2 directive. The Blueprint is thus not only the product of the convergence discourse, but also the catalyst for further integration and the establishment of new institutional structures. This process was triggered through the discourse initiated by a Member State perceiving the current structures to be dysfunctional.

The Blueprint is widely considered to be the most important step of European integration in the field of cyber crisis management. It not only lays out a comprehensive framework and mechanisms of how the fragmented cyber crisis management regime of the EU should coordinate in the case of a cyber crisis, but also led to the establishment of coordinated operational mechanism in the CyCLONe. In this way, it is linked to the evolution of the NIS 2 directive, viewed to be a next big step in coordinated cyber crisis management and shows that further European integration can happened through a discourse in which ideas of the functionality of existing institutional structures are challenged. As a perpetuation of the convergence discourse, it must also be seen as yet another steppingstone to the currently

evolving joint cyber unit (JCU) and the framework for strategic crisis management of the EU, which will be discussed in the 'outlook' chapter.

The Cyber Diplomacy Toolbox 2017

Before examining the Cyber Diplomacy Toolbox, it is important to stress, that the Toolbox is not synonymous to the practice of cyber diplomacy. While the Toolbox represents a sanctions regime, that is used for deterring adversaries, cyber diplomacy incorporates way more than responding to cyberattacks. Cyber diplomacy, as "[…] the use of diplomatic resources and the performance of diplomatic functions to secure national interests with regard to the cyberspace." (Barrinha & Renard, 2017, p. 355), is concerned with the geopolitical aspects of cyberspace. It complements technical capacities for addressing the increasingly contested nature of cyberspace and aims at managing cyberspace in relation to material implications in the physical world. The basis for the EU's cyber diplomacy is found in its Conclusions on Cyber Diplomacy of 2015 (Council of the European Union, 2015). In the context of the Cyber Diplomacy Toolbox however, cyberdiplomacy concerned with deterring adversaries by punishment through an elaborated and coordinated sanctions regime.

The Cyber Diplomacy Toolbox was initiated at the same time as the Blueprint and was introduced through different steps of integration of EU cybersecurity policy. In the same manner as the Blueprint, the Cyber Diplomacy Toolbox has its philosophical roots in the CSSEU. As previously mentioned, the CSSEU introduced the need for establishing EU cyber defence capacities, which then turned into the Cyber Defence Policy Framework in 2014. This framework set the basic strategic objectives for cyber defence and introduced a streamlining of cybersecurity policy into the CSDP structures, missions and operations. In the same way as the other EU document on cybersecurity the Cyber Defence Policy Framework has the underlying philosophy of the securitisation discourse (Council of the European Union, 2014). As the cybersecurity discourse evolved however, the idea was introduced, that defending cyberspace alone does not necessarily lead to a secure cyberspace. Due to the peculiarities of cyberspace, it becomes necessary to approach cybersecurity in a more comprehensive way and introducing measures for deterring adversaries was introduced as one of the main components. This idea was picked up by a supranational discourse and got turned into a joint communication on resilience, deterrence and defence in cyberspace (European Commission & High Representative, 2017). While the deterrence discourse emerged in the EU, the practice of cyber diplomacy was introduced through the *Conclusions on Cyber Diplomacy* of 2015. Additional to cyber diplomacy's tasks of forming international norms and building confidence with third

countries, the idea of cyber diplomacy taking on deterrence was introduced and led to the establishment of the Cyber Diplomacy Toolbox in 2017.

The Cyber Diplomacy Toolbox was established to create a framework for coordinated diplomatic response against malicious behaviour in cyberspace. It is a framework under the CFSP and includes measures that are "[…] proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity." (Council of the European Union, 2017). This may include the issuing of joint statements condemning behaviour to imposing restrictive measures. The mechanism of the Cyber Diplomacy Toolbox in the case of a cyber incident or cyber crisis is a four-stage process of preparing, attributing, decision making and communication. What is important to notice, that attribution in the process of responding to malicious cyber behaviour "[…] remains a sovereign political decision based on all-source intelligence." (Ibid., p. 4). This points to the great challenge of attribution in cyberspace and is linked to the notion of political attribution.

As deterrence has evolved as one of the main pillars of cyber defence policy, the Cyber Diplomacy Toolbox became the main instrument for deterrence (European External Action Service, 2022). In the context of cyber crisis management, deterrence is situated in the phases of prevention and response of the crisis management cycle. It is believed to be an appropriate mean to respond to and prevent cyber crisis. The rationale behind it is a prevention through punishment. The sanctions that are threatened to be imposed, deter an adversary to engage in malicious activities in the first place. In the case of a cyberattack, the sanctions regime is capable to inflict repercussions that stand as a precedent. The Cyber Diplomacy Toolbox is considered a sufficient offensive mean in the context of the EU's disinterest in fostering other, technical offensive capabilities (Interview 2). Some would even go as far as to frame Council conclusions to have a deterring effect. The communication of what the EU deems as acceptable state behaviour in space and introducing possible reactions are believed to carry deterring power (Interview 3).

The Cyber Diplomacy Toolbox was created out the discourse of deterrence, which it carries within. Built on the securitisation discourse it constitutes the need to "[…] protect the integrity and security of the EU, its Member States and their citizens against cyber threats and malicious cyber activities." (Council of the European Union, 2017, p. 2). It then goes on to define the problem of the "[…] willingness of State and non-state actors to pursue their objectives by undertaking malicious cyber activities of varying in scope, scale, duration,

intensity, complexity, sophistication and impact" (Ibid., p. 2) and introduces a solution through stressing that "[…] clearly signalling the likely consequences of a joint EU diplomatic response to such malicious cyber activities influences the behaviour of potential aggressors in cyberspace thus reinforcing the security of the EU and its Member States." (Ibid., p. 4). The Cyber Diplomacy Toolbox thus holds diplomatic sanctions, or the signalling of them to be an appropriate mean to deter potential adversaries to engage in malicious cyber activities aimed at the EU. This is based on the rationale that offensive capabilities must complement defensive means for comprehensively manage arising crisis in cyberspace. This begs the question why the EU does not engage in forging technical offensive capabilities. The discourse on deterrence argues for creating means that are most likely to deter adversaries, and in the logic of deterrence by punishment, means that do the outmost damage have a greater deterring effect. Diplomatic sanctions in this regard have arguably little consequences in comparison to capacities of engaging in offensive cybercampaigns that can attack an adversary's critical infrastructures and fundamentally disrupt the functioning of a state's political system, economy and society. Two explanations come to mind. First it is useful to reconsider the normative part of ideas and discourses. The reason why the EU does not engage in forging technical offensive capabilities is because this idea conflicts with the normative constellation of the EU. It devotes itself to the peaceful settlement of disputes in cyberspace and the responsible state behaviour in cyberspace (Council of the European Union, 2017, p. 3). This does not allow the EU to build an outright capability for engaging in offensive strategies in cyberspace. Secondly, the cognitive idea of building capable offensive measures may conflict with national discourses of sovereignty. As has been the case in CFSP/CSDP since their introduction, Member States are reluctant to confer competences to the supranational level due to a discourse on national sovereignty. The main provider of security within the EU remains the Member States, or within the context of other international organisations: NATO.

The Cyber Diplomacy Toolbox can thus be considered a contested mean of deterring adversaries in the cyber domain and contributing to cyber crisis management. This can for one be observed by the fact that only two years after the Cyber Diplomacy Toolbox was created, the European council established an own capacity to introduce sanctions (Council of the European Union, 2019). While basically following the same logic, a supranational discourse emerged containing the idea that an additional EU capacity is necessary. The Cyber Diplomacy Toolbox is the first policy manifestation of the discourse on deterrence, but may be considered an incomplete institutional change, because of the generally contested applicability of

deterrence in cyberspace, and its arguably very weak operationalisation. However, it still constitutes a step of European integration in the field of cyber crisis management, which due to its incompleteness already caused further institutional change.

Discussion of the Findings

The presented case study shows how European integration in the field of cyber crisis management was initiated and evolved over time. By applying the ex-ante established causal mechanism it is shown how the discourses of securitisation, convergence and deterrence have driven institutional change. The securitisation discourse was consolidated in the CSSEU. It is the underlying philosophy that is referred to in all the other EU documents and that caused the integration in the field of cyber crisis management. The process of integration was then driven by the discourses on convergence and deterrence. As they materialised in the form of the NIS Directive, the Blueprint and the Cyber Diplomacy Toolbox, they caused further integration by introducing new ideas of how to manage cyber crises, or through incomplete institutional reform.

The introduction of the NIS directive was initially hindered by a conflict of national and supranational discourses, but eventually led to further integration as a technical cooperation mechanism, was introduced that sparked the idea of an operational cooperation mechanisms to manage transboundary crisis. The Blueprint being the result of the discourse on convergence caused further integration by including an incomplete and dysfunctional version the aforementioned operational coordination mechanism. A new functional version of the mechanism was thus created, which also led to the proposal of the NIS 2 Directive. The Cyber Diplomacy Toolbox is a prime example of how conflicting cognitive and normative ideas lead to incomplete institutional reform. The programmatic discourse on deterrence calls for the establishment of offensive capabilities and the engagement in proactive strategies to comprehensively managing crisis in cyberspace. While developing offensive cyber capabilities or threatening a response through kinetic warfare would have the strongest deterring effect, the EU norm of peaceful conflict settlement conflicted with these endeavours. The EU thus decided to establish a coordinated sanctions regime, which was however again perceived to be an incomplete institutional reform as an EU sanctions capability was established only two years later.

These accounts confirm the applicability of the causal mechanism in tracing European integration in the field of cyber crisis management. It is shown that the underlying discourse

of securitisation, carrying a conceptualisation of cyber crises initiated the integration process, which was then driven by discourses of convergence and deterrence. Further integration happened, as incomplete institutional reforms were established due to conflicting supranational and national discourses, as well as conflicting normative and cognitive ideas. The process furthermore followed the logic of institutional layering.

Chapter 5: The Future of EU Cyber Crisis Management

The existing cyber crisis management regime of the EU is highly fragmented which some authors argue render the EU an incapable transboundary crisis manager or (cyber-)security actor. The case study of this thesis however shows a clear trend of accelerating integration in the fields of cyber crisis management and cybersecurity policy as a whole. The Blueprint must be seen as the most important catalyst of integration as it has put strategic and comprehensive transboundary crisis management at the top of the agenda of the EU. This overarching trend can be observed by looking the priorities of the von der Leyen Commission, which even introduced a new commissioner exclusively responsible for crisis management (European Commission, 2022). In addition to this overarching discourse, a few more particular steps of integration can be observed in the field of cyber crisis management, driven by the discourses on convergence and coherence.

First, the European Commission issued a recommendation on building a Joint Cyber Unit (JCU). In their recommendation the Commission stressed the importance of cybersecurity to a digital transformation, points to the cyber vulnerabilities that have been made obvious by the COVID-19 Pandemic and recognises the trans-national nature of cybersecurity threats, incidents. The JCU is the Commission's attempt to establish an overarching framework of existing capabilities across the four existing cyber communities. One of the JCU's main task will be to establish a European cybersecurity crisis management framework, that will identify risks and threats, mitigate and respond to them in a coordinated and timely fashion (European Commission, 2021a).

Secondly, the Commission released a scoping paper on the strategic crisis management in the EU. In the face of possible future natural or human-made systemic shocks, the Group of Chief Scientific Advisors (GCSA) is asked to produce a scientific advice on how the EU can improve its strategic crisis management. The advice should address added value of new policies, clarity of concepts as risks, emergencies, disasters, crisis, and possible improvements to an overarching crisis management framework. The case studies shall include climate change,

cross-border health threats and large-scale cybersecurity threats. The scientific sill be delivered to the commission at the end of Q2 in 2022 (European Commission, 2021c). Both documents are emblematic of the EU's

Thirdly, an example for the continuation of the deterrence discourse can be found in the Strategic Compass of 2022. After reinforcing the necessity and applicability of the Cyber Diplomacy Toolbox, the Strategic Compass commits the Union to create a "Hybrid Toolbox" along with "Hybrid Rapid Response Teams". Both are aimed to deter and respond to incurring hybrid threats and raise the EU's capability of transboundary crisis management. Furthermore, cybersecurity policy will in the future be streamlined into the EU's general crisis management capabilities in the context of CSDP missions (Council of the European Union, 2022a). A clear continuation of the deterrence, as well as the convergence discourse can be found in the Strategic Compass, which sets out steps for further integration.

These developments are only some examples of how the EU's cyber crisis management regime is currently evolving. Others include the provisional agreement on a NIS 2 directive (Council of the European Union, 2022b) and the proposal for a directive on the resilience of critical entities (European Commission, 2020). Overall, the current developments give us a hunch about the direction of European integration in the field of cyber crisis management and let us speculate on the future capabilities of the EU to manage cyber crisis.

The EU as a Capable Cyber Crisis Manager

The discussion on the capability of the EU as a cyber crisis manager has to date been a theoretical one. Scholars have given their assessments on the EU as a cyber security actor and a transboundary crisis manager by examining EU structures and modes of governance. However, the fact that there has not been a cyber crisis yet, lets us not draw conclusions based on empirical evidence. One indication of the functionality of cyber crisis management capabilities was the large-scale exercise conducted under the French presidency of the Council of the EU in the first half of 2022. A cyber crisis was simulated to examine the interaction of the multiple actors across communities, structures of coordination and crisis response mechanisms. The exercise was successful in the way that existing standardised processes are functioning in the way they were designed. The EU's capability of managing cyber crisis is heavily reliant on its Member States' capabilities, who are the responsible actors for cyber crisis management. As crisis management is a national responsibility and technical and operative resources are primarily situated within the Member States, the supranational level

can only facilitate the coordinated management. The question if the EU is a capable cyber crisis management actor thus remains, for the time being a hypothetical one (Interview 5).

When discussing the ability of the EU to manage crisis in cyberspace, a question worth asking is: does the EU have to be a capable cyber crisis management actor? The question comes in relation to the other international organisation, that are engaged in managing crisis in cyberspace, namely the OSCE, NATO and the UN. The OSCE is an international organisation that heavily engages in confidence building measures (CBMs) to prevent cyber crisis from eroding. Based on information sharing, norm creation and mutual capacity building, CBMs render the OSCE to possibly be the most important international actor in managing crisis in cyberspace. This is furthermore related to its approach of communication in times of crisis. The OSCE is a platform where adversaries can communicate in an international environment without being scrutinised by public opinion. As attribution is one of the biggest challenges in cyberspace, engaging with possible adversaries, to bridge the gaps and foster cooperation must be perceived as a very valuable tool in managing cyber crises. (Interview 4). Furthermore, the EU's approach of deterring adversaries by employing a sanctions regime is a contested endeavour on its own. When putting it into the context of NATO however, it becomes even more questionable. NATO stated that a cyberattack can be grounds for joint military action under the scope of collective defence. The threat of engaging in kinetic warfare if deemed necessary holds in deterrence terms way bigger significance than imposing restrictive measures.

Does this mean that all of the EU's efforts in engaging in comprehensive crisis management must be deemed insufficient and pointless? I argue no. Even though the EU deploys fragmented means in managing cyber crisis that involve huge bureaucratic efforts and are hindered by many different factors, it still manages to provide valuable capabilities within its own scope. The EU as a project has always had great ambitions. In the context of a currently accelerating integration process in the cyber domain, linked to an evolving security identity, the time is right for pushing the EU's cyber crisis management capabilities even further. The EU is however well advised to be aware of its institutional limitations and would benefit from following the examples from other international organisations. The EU can especially learn from the OSCE in their efforts of building confidence across ideational frontiers. Engaging in dialogue has great potential in mitigating arising crisis, which holds especially true for the cyber domain. The EU should thus focus its cyber diplomatic efforts that are not related to issuing sanctions.

Conclusion

By applying the approach of discursive institutionalism (DI) this thesis has shown that European integration process in the field of cyber crisis management was initiated by a securitisation discourse, containing the conceptualisation of a cyber crisis. It also showed how salient discourses have shaped the integration dynamics and led to the evolution of the currently existing cyber crisis management regime (CCMR) of the EU.

The thesis in its first part has established how discourses can cause intuitional change and introduced a causal mechanism for European integration. The discourses of securitisation, convergence and deterrence were then derived from examining the particularities of cyberspace and cyber crisis and introduced to the causal mechanism. The case study of part two then revealed that the integration process in the field of cyber crisis management was initiated by an underlying, philosophical discourse of securitisation and then perpetuated by the discourses on convergence and deterrence. Furthermore, institutional change was the result of incomplete institutional reform, related to conflicting national and supranational discourses and incompatible cognitive and normative ideas. The examined cyclical process of integration can furthermore be examined to follow the logic of institutional layering.

This thesis has contributed to the existing literature on European integration and the EU's cyber crisis management in two ways. Firstly, it has established, that European integration may happen without a crisis. In the case of the integration in the field of cyber crisis management, the mere conceptualisation of a cyber crisis was enough to trigger a cyclical process of institutional change. This thesis is thus an account of the explanatory power of discourses in European integration and provides an alternative to neofunctionalist and liberal intergovernmentalist approaches. Secondly, this thesis has established a causal mechanism that can trace European integration without the necessity of a crisis or an incurring shock. This mechanism has great potential of being applied in other policy areas to European integration.

The effectiveness of the EU's cyber crisis management regime remains to be seen. Approaches of convergence deem the EU incapable of managing cyber crisis and deterrence remains a highly contested strategic approach. The EU however shows great potential in maximising the effectiveness of its limited role. It is well advised to cooperate with and learn from its international partners and foster international norms in cyberspace to mitigate cyber crisis before they arise. Only time will tell if the EU is a capable cyber crisis manager, although we may hope to never find out.

References

Ansell, C., Boin, A., & Keller, A. (2010). Managing Transboundary Crises: Identifying the Building Blocks of an Effective Response System. *Journal of Contingencies and Crisis Management*, *18*(4), 195–207. https://doi.org/10.1111/j.1468-5973.2010.00620.x

Backman, S. (2021). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management*, *29*(4), 429–438. https://doi.org/10.1111/1468-5973.12347

Backman, S., & Rhinard, M. (2018). The European Union's capacities for managing crises. *Journal of Contingencies and Crisis Management*, *26*(2), 261–271. https://doi.org/10.1111/1468-5973.12190

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4-5), 353–364. https://doi.org/10.1080/23340460.2017.1414924

Bergmann, J., & Müller, P. (2021). Failing forward in the EU's common security and defence policy: the integration of EU crisis management. *Journal of European Public Policy*, *28*(10), 1669–1687. https://doi.org/10.1080/13501763.2021.1954064

Biermann, F., Guérin, N., Jagdhuber, S., Rittberger, B., & Weiss, M. (2019). Political (non-)reform in the euro crisis and the refugee crisis: a liberal intergovernmentalist explanation. *Journal of European Public Policy*, *26*(2), 246–266. https://doi.org/10.1080/13501763.2017.1408670

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3), 449–464. https://doi.org/10.1111/gove.12309

Boin, A., Busuioc, M., & Groenleer, M. (2014). Building European Union capacity to manage transboundary crises: Network or lead-agency model? *Regulation & Governance*, *8*(4), 418–436. https://doi.org/10.1111/rego.12035

Boin, A., Rhinard, M., & Ekengren, M. (2014). Managing Transboundary Crises: The Emergence of European Union Capacity. *Journal of Contingencies and Crisis Management*, n/a-n/a. https://doi.org/10.1111/1468-5973.12052

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *JCMS: Journal of Common Market Studies*, *55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111–1126. https://doi.org/10.1080/07036337.2020.1853122

Christou, G. (2019). The collective securitisation of cyberspace in the European Union. *West European Politics*, *42*(2), 278–301. https://doi.org/10.1080/01402382.2018.1510195

Council of the European Union. (2014, November 18). *EU Cyber Defence Policy Framework* (15585/14). https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

Council of the European Union. (2015, February 11). *Draft Council Conclusions on Cyber Diplomacy* (6122/15). https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

Council of the European Union. (2017, June 19). *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* (10474/17). http://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf

Council of the European Union. (2019, May 14). *Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States* (7299/19). http://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf

Council of the European Union. (2022a, March 21). *A Strategic Compass for Security and Defence. For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security* (7371/22). https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

Council of the European Union. (2022b, June 17). *Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, abrogeant la directive (UE)* (10193/22). https://data.consilium.europa.eu/doc/document/ST-10193-2022-INIT/x/pdf

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93–125. https://doi.org/10.1111/rmir.12169

European Commission. (2001, June 6). *Communication on Network and Information Security: Proposal for A European Policy Approach* (COM(2001)298 final).

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298&from=EN

European Commission. (2010a, May 19). *Communication on A Digital Agenda for Europe* (COM(2010)245 final). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

European Commission. (2010b, November 22). *Communication on the EU Internal Security Strategy in Action: Five steps towards a more secure Europe* (COM(2010) 673 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673&from=EN

European Commission. (2017). *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises.* European Commission. https://www.notion.so/Blueprint-b8ee75e062664b608f35acf95017cd5d

European Commission. (2020). *Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities COM (2020) 829 final*. https://www.notion.so/DIRECTIVE-on-the-resilience-of-critical-entities-ef1631bf4563460286b3684d49d2b6be

European Commission. (2021a). *Commission Recommendation on building a Joint Cyber Unit* [EU 2021/1086]. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021H1086&from=EN

European Commission. (2021b). *Factsheet: Joint Cyber Unit*. Publications Office of the European Union.

European Commission. (2021c, June 22). *Strategic crisis management in the EU: Improving EU crisis prevention, preparedness, response and resilience*. https://ec.europa.eu/info/files/scoping-paper-strategic-crisis-management-eu-june-2021_en

European Commission. (2022). *Janez Lenarčič: Crisis Management*. https://ec.europa.eu/commission/commissioners/2019-2024/lenarcic_en

European Commission, & High Representative. (2013, February 7). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013) 1 final). https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission, & High Representative. (2017, September 13). *Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*

(JOIN(2017) 450 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

European External Action Service. (2022, March 21). *Questions and answers: a background for the Strategic Compass*. https://www.eeas.europa.eu/eeas/questions-and-answers-background-strategic-compass_en

European Union. (2016, July 6). *Directive concerning measures for a high common level of security of network and information systems across the Union* (2016/1148). European Parliament; Council of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Fahey, E. (2020). Institutionalising EU Cyber Law: Can the EU institutionalise its many subjects and objects? *Working Paper Series*(2020/1), 1–37.

Fischerkeller, M., Harknett, R., & Vićić, J. (2020). The Limits of Deterrence and the Need for Persistence. In A. F. Brantly (Ed.), *The Cyber Deterrence Problem* (pp. 21–38). Rowman & Littlefield International.

Globe. (2020). *NATO/EU/OSCE Membership overlap*. https://www.globe-project.eu/en/nato-eu-osce-membership-overlap_11001#:~:text=The%20member%20states%20that%20are%20only%20a%20member%20of%20NATO,also%20participate%20in%20the%20OSCE.

Gursch-Adam, R. (2022, June 9). *The Rule of Law in the Context of Cyber Security and Hybrid Threats: An overview on issues of International Law in cyber operations.* Austrian Institute for European and Security Policy.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Harknett, R., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 1–34. https://doi.org/10.1080/01402390.2020.1732354

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

Hyde-Price, A. G. V. (2001). "Beware the Jabberwock!": Security Studies in the Twenty-First Century. In H. Gärtner (Ed.), *Europe's new security challenges* (pp. 27–54). Rienner.

Jones, E., Daniel Kelemen, R., & Meunier, S. (2021). Failing forward? Crises and patterns of European integration. *Journal of European Public Policy*, *28*(10), 1519–1536. https://doi.org/10.1080/13501763.2021.1954068

Krepinevich, A. F., Jr. (2019). The Eroding Balance of Terror: The Decline of Deterrence. *Foreign Affairs*, *98*(1), 62.

Lancelot, J. F. (2020). Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, *4*(4), 240–254. https://doi.org/10.1080/23742917.2020.1798155

Lanzara, G. F. (1998). Self-destructive processes in institution building and some modest countervailing mechanisms. *European Journal of Political Research*, *33*(1), 1–39. https://doi.org/10.1111/1475-6765.00374

Lauth, H.-J., Kneuer, M., & Pickel, G. (2016). *Handbuch Vergleichende Politikwissenschaft*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-02338-6

Lavenex, S. (2018). 'Failing Forward' Towards Which Europe? Organized Hypocrisy in the Common European Asylum System. *JCMS: Journal of Common Market Studies*, *56*(5), 1195–1212. https://doi.org/10.1111/jcms.12739

Lefkofridi, Z., & Schmitter, P. C. (2015). Transcending or Descending? European Integration in Times of Crisis. *European Political Science Review*, *7*(1), 3–22. https://doi.org/10.1017/S1755773914000046

Mahoney, J., & Thelen, K. A. (2010). *Explaining institutional change: Ambiguity, agency, and power*. Cambridge University Press. https://doi.org/10.1017/CBO9780511806414

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, *75*(4), 432–459. https://doi.org/10.1080/10357718.2021.1926423

Nye, J. S. (2010). *Cyber Power*. Belfer Center for Science and International Affairs.

Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security*, *26*(2), 87–102. https://doi.org/10.1162/016228801753191141

Prevezianou, M. F. (2021). Beyond Ones and Zeros: Conceptualizing Cyber Crises. *Risk, Hazards & Crisis in Public Policy*, *12*(1), 51–72. https://doi.org/10.1002/rhc3.12204

Provan, K. G., & Kenis, P. (2007). Modes of Network Governance: Structure, Management, and Effectiveness. *Journal of Public Administration Research and Theory*, *18*(2), 229–252. https://doi.org/10.1093/jopart/mum015

Schimmelfennig, F. (2015). Efficient process tracing: Analyzing the causal mechanisms of European integration. In A. Bennett & J. T. Checkel (Eds.), *Process Tracing: From Metaphor to Analytic Tool* (pp. 98–125). Cambridge University Press.

Schmidt, V. A. (2008). Discursive Institutionalism: The Explanatory Power of Ideas and Discourse. *Annual Review of Political Science*, *11*(1), 303–326. https://doi.org/10.1146/annurev.polisci.11.060606.135342

Tagarev, T., & Ratchev, V. (2020). A Taxonomy of Crisis Management Functions. *Sustainability*, *12*(12), 5147. https://doi.org/10.3390/su12125147

Trimintzios, P., Ogee, A., Gavrila, R., & Zacharis, A. (2015). *Report on cyber crisis cooperation and management: Common practices of EU-level crisis management and applicability to cyber crises*. ENISA.

van der Meer, S. (2016). Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity. In C. Samuel & M. Sharma (Eds.), *Securing Cyberspace: International and Asian Perspectives* (pp. 95–105). Pentagon Press.

Institutional Affiliation of Interviewees

Interview 1	European Commission
Interview 2	European Defence Agency
Interview 3	Austrian Ministry for European and International Affairs
Interview 4	Austria Institute for European and Security Policy
Interview 5	Austrian Federal Chancellery