

Virtually inconceivable: Ontological insecurities and the rise of geopolitics and sovereignty in EU cybersecurity policy

---

A thesis submitted to the Postgraduate Programme of the Department of Politics and International Relations in partial fulfilment of the requirements for the Degree of Master of Philosophy in Politics: European Politics and Society at the University of Oxford

Julia Carver
Word Count: 29,990

Thursday, 20 May 2021

Department of Politics and International Relations
University of Oxford

Trinity Term 2021

Acknowledgements

To my family

I would like to express my deepest gratitude to the policy practitioners who devoted their precious time and energy as interviewees for this research project—your openness, patience, and insights were invaluable for my research.

I would also like to thank my supervisor, Dr Robert Johnson, who has always believed in my ideas from the start, provided me with critical support and feedback during the toughest points of this project, offered me many opportunities to engage with my research outside of the (virtual) classroom—and who never failed to lift my spirits, even across a computer screen.

Above all, this dissertation would not have come to fruition without the support and kindness of my friends and family. First and foremost, to Emerson—thank you for giving me confidence and crucial advice when I needed it the most. Thijs, thank you for your endless patience, your listening ear, and your unwavering belief in my capacity to finish this project—you were always holding the light at the end of the tunnel. To my course mates—I could not have been luckier to undertake research with such an incredible group of people, who never failed to resurrect my motivation and keep things 'light' throughout the most difficult moments of the pandemic. And finally, to my parents and to my sister, Katrina—your unconditional love and understanding made me feel as if there had not been an ocean between us. Thank you for always believing in my ability to undertake this degree, especially during times when I did not. Thank you to all the wonderful people who helped me along this journey—without you, I could not have reached my destination.

Abstract

The policy domain of cybersecurity has become inundated with geopolitical concepts and sovereignty appeals over the last decade, arousing the interest of scholars and policymakers alike regarding how such a notable shift has implicated the behaviour of actors in cyberspace. Scholarship conventionally expects state actors with cyberwarfare and intelligence capabilities to voice geopolitical reasoning and sovereigntist claims, overlooking the presence of such discourse within the European Union's (EU) cyber policies. Yet, the EU's agenda of 'technological sovereignty' and its invocation of geopolitical metaphors have become increasingly prevalent in its cybersecurity policy, whereupon 'European sovereignty' has emerged as a priority—defying expectations based upon the EU's traditional eschewal of geopolitics, and scholarly assumptions about its capabilities as a cyber actor.

Thus, to explore this development, I ask how, and why, such geopolitical and sovereigntist language has emerged in EU cybersecurity policy, and the implications of such language upon the EU's self-conception as a cyber actor. Adhering to an interpretive-qualitative methodology, I develop a chronology of EU cybersecurity policy development from 2009-2020 and conduct discourse analyses of documents and elite interviews. My dissertation undertakes a sustained focus upon the ontological dimension to cyber policymaking, particularly ontological insecurity—an approach not yet leveraged in this empirical context. Through the lens ontological insecurity, I argue that the emergence of geopolitical and sovereigntist language in EU cybersecurity policy is a consequence of how EU cybersecurity policy has centred upon the management of particular ontological insecurities in cyberspace, for which policymakers have leveraged discursive strategies oriented around the delegitimization, and later legitimization, of geopolitics. Sovereignty, in turn, emerged as a response to insecurities elicited by the EU's decision to 'speak in geopolitical terms', and has become prevalent as a means of differentiating the EU from geopolitical actors in cyberspace.

Overall, my dissertation illustrates how insecurities about the EU's past, cyberspace as an environment, and relations with cyber actors have shaped the dominant ideas and policy responses over the course of 2009-2020, enabling the emergence of sovereigntist and geopolitical language in this contemporary stage of the EU's development. Significantly, it unmasks a key tension underlying EU cybersecurity policy: while the EU has increasingly articulated traditional, state-centric assumptions about geopolitics in cyberspace; simultaneously, EU policymakers have sought to represent the EU as transcendent of this dynamic for which the vocabulary of 'European sovereignty' has been leveraged to differentiate the EU from geopolitical actors in cyberspace.

TABLE OF CONTENTS

Chapter I - Introduction 6
Overview of Study 9
Chapter Summary 10
Chapter II - Review of the Literature 13
Cyber Policymaking Challenges 13
Acting Upon Ontologies 19
Expressing Ontologies 23
The Ontological Dimension to Cybersecurity Policy 26
Chapter III – Theory and Methods 29
Theoretical Approach 29
Interplay with Securitization 35
Responding to Ontological Insecurities 37
The Delegitimization of Geopolitics: Temporal Othering 38
Relational and Spatial Othering 39
The Legitimization of Geopolitics in EU Cyber Policy 42
Methodology and Research Design 44
Discourse-Analytical Method 48
Document Analysis 49
Interviews 51
Conclusion 54
Chapter IV - Delegitimization 55
The Securitization of Cyberspace 55
The Estonia Cyberattacks 56
Autobiographical Insecurities 60
Cybersecurity in the Union: A Humble Beginning 67
The Delegitimization of Geopolitics 68
Conclusion 70
Chapter V – Rupture and Reconceptualization 72
Erupting Insecurities: The Ukraine Crisis 73
Spatialization and Externalisation in Cyber Capacity Building 80
Rupture 86
Reconceptualization 89
Conclusion: Towards European Sovereignty in Cyberspace 92
Chapter VI – Legitimization and European Sovereignty 94
From Awareness to Action 95
Diktat Anxieties (5G), Weaponizing Interdependencies, and Transatlantic Implications 96
The Emergence of Sovereignty in EU Cybersecurity Policy 104
European Sovereignty as a Form of Differentiation 107
The Spectre of Geopolitics 107

Responding to Geopolitics with European Sovereignty 111
A Strong Foundation? 114
Conclusion 117
Chapter VII – Conclusion 119
Bibliography 128
Appendices 140
Appendix 1 – Literature Review (Chapter 2) 140
Appendix 2 – Methodology (Chapter 3) 141
Appendix 3 –Legitimization and European Sovereignty (Chapter 6) 142
Appendix 4 – List of Primary Textual Sources Cited* 145

LIST OF FIGURES

Figure 1. Various loci of ontological insecurities in EU cyber policy discourse. 34
Figure 2. Central pillars of EU cybersecurity strategy (2013), as compiled by George Christou. 48
Figure 3. Interviewees' affiliations to EU cyber policy communities. 52
Figure 5. An EU Commission visualization of worldwide cyberattacks in 2016. 79
Figure 4. Current map of the CyberEast partnership region. 84
Figure 6. EU Commission diagram on 'What 5G is about' (2020). 97
Figure 7. Relational Othering in EU cyber policy discourse. 111

LIST OF TABLES

Table 1. Theorized ontological insecurity responses. 38
Table 2. WPR Analysis (Bacchi and Goodwin, 2016). 50

‘Whoever fights monsters should see to it that in the process he does not become a monster. And if you gaze long enough into an abyss, the abyss will gaze back into you.’

Friedrich Nietzsche (1886)

‘The advent of the digital age is often equated with the rise of Silicon Valley, but extraordinary although that is, its true origins lie in geopolitics and political power – to which it constantly returns.’

Anthony Giddens (2020)

Chapter I - Introduction

In December 2020, on the heels of a highly digitized year, the European Union (EU) released its updated cyber strategy, *The EU's Cybersecurity Strategy for the Digital Decade,* which re-asserted the imperative for the EU to strike a balance between '*technological sovereignty* and the need for international cooperation at the same time.[1] The penholders of this bold approach are the heads of EU's new 'geopolitical commission': Ursula von der Leyen, the EU Commission President, and Joseph Borrell, the High Representative (HR/VP) of the External Action Service. The significance of Brussels' official declaration that European sovereignty should be a defining objective and priority for 'the digital decade' is not confined to the policy area of cybersecurity. Rather, it reflects HR/VP Borrell's overall mission for 'the EU [to] learn the language of power and act geopolitically.'[2]

Strikingly, the EU's contemporary embrace of sovereignty and geopolitical language deviates from the Union's historical approach to these concepts in its official discourses, defying scholarly accounts about the EU as a political entity and as well as a cyber actor. On the one hand, the EU's *eschewal* of geopolitics and geopolitical language to explain its policies is widely considered to be a central premise of its 'founding myth.' Under the auspices of its 'virgin birth' as a supranational organization, the EU forswore traditional forms of geopolitics to frame itself as a post-Westphalian success story.[3] As Stefano Guzzini puts it, 'the EU has staked its reputation on being an anti-geopolitical unit …a peace organization, a "civilian" or "normative" power, aimed precisely at overcoming the militarism and nationalism historically associated with classical geopolitical thought that had plagued Europe's early twentieth

[1] European Commission and HRVP, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: The EU's Cybersecurity Strategy for the Digital Decade*, (Brussels, 2020), https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.

[2] As interviewed in Joseph Weiler, "Europe Must Learn Quickly to Speak the Language of Power," *EJIL: Talk! Blog of the European Journal of International Law*, October 29, 2020, https://www.ejiltalk.org/europe-must-learn-quickly-to-speak-the-language-of-power-part-i/.

[3] Nora Fisher Onar and Kalypso Nicolaïdis, "The Decentring Agenda: Europe as a Post-Colonial Power," *Cooperation and Conflict* 48, no. 2 (2013): 283–303, https://doi.org/10.1177/0010836713485384; Gabrielle Nicolaïdis, Kalypso, Sebe, Berny, Maas, *Echoes of Empire: Identity, Memory and Colonial Legacies*, 2015, www.ibtauris.com; Jan Zielonka, *Europe as Empire: The Nature of the Enlarged European Union*, vol. 9780199292 (Oxford University Press, 2006), https://doi.org/10.1093/0199292213.001.0001.

century.'[4] Yet, this contemporary discursive shift would suggest that the EU has *not* overcome classical geopolitical concepts identified with the Westphalian nation-state. On the contrary, it has become legitimized under Von der Leyen's geopolitical commission.

Secondly, the emergence of European sovereignty and geopolitical discourse in the cybersecurity context ruffles scholarly expectations about the EU as a cyber actor. Conventional accounts position Europe (especially the EU) as ancillary to the competing US-China power struggle for geopolitical and technological superiority in cyberspace. 'Cyber*space*' is thus bifurcated into two competing technological spheres of influence, within which an external (American or Chinese) power has control of the sphere's technology. As the 'technological crescent' over which those two powerful states struggle for dominance, Europe—and the EU—is seen as unable and *unfit* to pursue geopolitical interests.[5]

Yet, examining the EU's policy evolution in cyberspace more closely reveals important nuances and complications to this straightforward, 'power-politics' account of global geopolitical dynamics. While it lacks the expected trappings of a 'geopolitical power' or security player (namely, an intelligence arm and cyberwarfare capabilities), the EU has nevertheless established its own dedicated 'geopolitical commission' and its desire to 'speak in geopolitical terms.' Furthermore, the EU has advanced its own policies and development projects into geopolitically significant regions, exemplified by its funding of 'CyberEast' programmes in its Eastern Neighbourhood.

Additionally, the EU's recent assertion of *European* sovereignty compared to its earlier invocation of *national sovereignties* in official contexts should not be understated. *European technological sovereignty* has become one of the key priorities for the EU in the

[4] Stefano Guzzini, *The Return of Geopolitics in Europe?: Social Mechanisms and Foreign Policy Identity Crises* (Cambridge: Cambridge University Press, 2012), 6, https://doi.org/doi:10.1017/CBO9781139225809.

[5] Krzysztof Feliks Sliwinski, "Moving beyond the European Union's Weakness as a Cyber-Security Agent," *Contemporary Security Policy* 35, no. 3 (2014): 468–86, https://doi.org/10.1080/13523260.2014.959261; Valentin Weber, "Making Sense of Technological Spheres of Influence" (London, 2020), https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Technological-Spheres-of-Influence.pdf.

contemporaneous 'digital decade', in which it aims to ensure 'Made in Europe' solutions and its position as a technological leader.[6] Therefore, in light of the EU's assertive foreign policy and security approach to cyberspace, it would be appropriate to move beyond a perspective of global cyber politics as consisting of 'greater power' competition between China and the US to a more expansive one. Thus far, the link between geopolitical and sovereignty discourses to the EU's cybersecurity approach has remained critically underexplored.

In attempt to make sense of this discursive shift in EU cybersecurity policy, this thesis concerns itself with understanding how the EU – in spite of its traditional eschewal of geopolitics—has adopted geopolitical and sovereigntist language in official EU cybersecurity policies. Specifically, it asks two related questions:

1. How and why have geopolitical and sovereigntist discourses come to prevail in contemporary EU cybersecurity policy? and
2. How has this process shaped the EU's self-conception as a cyber actor?

There are significant empirical and theoretical imperatives for undertaking this research agenda. First, uncovering the interplay between geopolitical language and the EU's cybersecurity strategy expands our understanding of how cybersecurity is understood and practiced by non-traditional cyber actors and beyond the conventional American, Russian, and Chinese cases. Second, extant studies have generally focused on the inadequacy of using geopolitical and sovereigntist concepts for cybersecurity policymaking, rather than 'on what political work these forms of reasoning perform.'[7] In seeking to uncover the latter, and by examining the EU as an underexplored empirical case, my research contributes both to EU studies on cybersecurity, and the nascent fields of cyber-IR and -politics.

[6] European Commission, *Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Proposal for a Regulation of the European Parliament and of the Council. COM(2018) 630 Final 0328,* no. September (2018).

[7] Tim Stevens, *Cyber Security and the Politics of Time*, *Cyber Security and the Politics of Time* (Cambridge: : Cambridge University Press, 2016), 17, https://doi.org/10.1017/CBO9781316271636.

Overview of Study

This thesis develops a theoretical framework of *ontological insecurity* to answer its central research questions and adopts an interpretive-qualitative approach to draw out the 'meanings' of geopolitics and sovereignty as they have been metaphorically represented, understood, and applied in the context of the EU's cybersecurity policy environment. Ontology refers to the assumptions or claims one makes about *being,* about 'what *is* […], what e*xists*,' and about 'the constituent units of reality.'[8] My study therefore foregrounds the importance of language as *foundational*—not only functional—to the EU's development;[9] 'as an instrument of will and intention' in the words of Thomas Diez.[10]

The central argument of this dissertation is that the EU's discursive engagement with geopolitical concepts and appeals to sovereignty can be understood as distinctive responses to the EU's growing ontological insecurities in cyberspace. These responses were dominated by various strategies of 'othering', centred upon managing insecurities about the EU's autobiographical self, its surrounding spatial environment, and its security relative to others in cyberspace. Over time, these responses led to the legitimization of geopolitics in EU official discourses and policymakers' adoption of 'European sovereignty' to construct the EU's identity as a cyber actor.

This study focuses upon the ideational and political context in which geopolitical and sovereigntist language has been discussed by EU policymakers over time. Rather than uncovering the 'facts' about 'geopolitics' in the EU, it examines how the concepts of sovereignty and geopolitics 'function in political debates and how [they] enable particular territorial conceptions of security.'[11] The distinctive meanings of 'geopolitics' and '*European*

---

[8] Colin Hay, "Political Ontology," in *The Oxford Handbook of Political Science*, ed. Robert E. Goodin (Oxford University Press, 2011), https://doi.org/10.1093/oxfordhb/9780199604456.013.0023.

[9] Pertti Joenniemi, "Re-negotiating Europe's Identity: The European Neighbourhood Policy as a Form of Differentiation," *Journal of Borderlands Studies* 23, no. 3 (2008): 83–94, https://doi.org/10.1080/08865655.2008.9695710.

[10] Thomas Diez, "Speaking 'Europe': The Politics of Integration Discourse," *Journal of European Public Policy* 6, no. 4 (1999): 601, https://doi.org/10.1080/135017699343496.

[11] Merje Kuus, *Geopolitics Reframed : Security and Identity in Europe's Eastern Enlargement* (Ebook: Palgrave Macmillan US, 2007), 6.

sovereignty' as they have been expressed in the EU context are uncovered by this study's interpretive analyses of textual sources and interview responses.

Undertaking this research responds to calls for further theoretical engagement with the ontological foundations of cybersecurity as a practice.[12] Empirically, this study examines the EU's cybersecurity development as a novel empirical case of how individuals (EU policymakers) have reimagined the political identity of a collective actor after a period of existential crisis. Ultimately, this study endeavours to peel back the multi-layered discursive dynamics of EU cybersecurity policy development to date, which may contribute to a clearer understanding of how particular conceptions of cyberspace can not only influence perceptions of security, but they may also precipitate the emergence of particular *concepts* in EU policy discourse. For policymakers, it uncovers what the concepts of 'European sovereignty' means for the Union and situates this conceptualization within the broader global context of 'moving geopolitical plates.' This is of utmost contemporary importance—as two EU officials emphasized to me, understanding actors' conceptions of 'cybersecurity' and 'sovereignty' is critical for conducting international relations in cyberspace, given the diversity of existing global approaches to these key tenets of politics and international relations.[13]

Chapter Summary

In the following Chapter (II), I conduct a review of the literature on cyber politics and international relations and delineate how extant scholarship has established, albeit equivocally, that policymakers experience acute ontological insecurities in cyberspace. Specifically, I argue that conventional materialist/realist approaches are incapable of fully explaining the EU's adoption of geopolitical and sovereigntist language on the basis that they reproduce the very ontological assumptions that merit critique in this context. I then consider the insights of

[12] Tobias Liebetrau and Kristoffer Kjærgaard Christensen, "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites and Spaces," *European Journal of International Security*, 2020, 1–19, https://doi.org/10.1017/eis.2020.10.

[13] Interviewee A, interview by author, virtual (online video), March 5, 2021. Also expressed by interviewee D, interview by author, virtual (online video), March 18, 2021.

ideational and interpretivist approaches to cybersecurity, which suggest that a discursive-analytic approach could better grapple with these tensions.

Next, in Chapter III, I lay out my theoretical approach on ontological insecurity and the central tenets of my argument, which holds that the EU's contemporaneous adoption of geopolitical and sovereigntist language is driven by policymakers' various responses to ontological insecurities in cyberspace over time. Based upon my interpretive analysis, I theorize that three primary strategies were employed by policymakers over the course of the EU's cyber policy development: *temporal, relational*, and *spatial othering*. Subsequently, I lay out my interpretive-qualitative research design and methodology, which is centred upon the discursive analysis of textual sources and interviews with EU policymakers.

In Chapters IV-VI, I present my empirical argument in chronological order, which is periodized in line with the release of the EU's three cyber strategies: 2009-2013; 2014-mid 2017; and late 2017-2020. Chapter IV traces the rise of securitization in EU cyber policy and how this process facilitated the further ideational convergence of EU cyber discourses with the domain of security policy more broadly. During this period, which culminated with the release of the EU's debut cybersecurity policy in 2013, the Union's strategy of mitigating its autobiographical insecurity was characterized by the delegitimization of geopolitical ideas and an inward-looking security focus. Subsequently, Chapter V argues that the 2014-mid 2017 period was one of 'ontological rupture' for the EU. Several transformative events propelled the EU into an identity crisis, driving it to engage in two additional strategies to mitigate its ontological insecurities: spatial and relational othering. Collectively, these events precipitated the reconceptualization of the EU's role as a global actor, which deeply impacted the trajectory of EU cybersecurity policy. Cyber policy began to reproduce the spatial and relational concepts laid out by the EU's new global outlook, paving the way for the legitimization of geopolitics. Next, Chapter VI explores the emergence of geopolitical and sovereigntist language into the

EU's most recent cybersecurity policies and threat representations. It argues that the EU's adoption of 'European sovereignty' in cybersecurity policy was not only the result of cyber policy's conceptual integration with the EU's global outlook—rather, it was a response to policymakers' anxieties about speaking in geopolitical terms, operating as a way to differentiate the EU from other actors. Moreover, while Brussels has advanced 'European sovereignty' as a distinctive new cyber policy objective abroad, internal contestation has destabilized this aspect of the EU's self-conception.

In Chapter VII, I consider the implications of the EU's adoption of geopolitical and sovereigntist language in its official cybersecurity policy and highlight the significant tensions which have emerged from this development. I conclude that this dissertation offers a preliminary point of departure for exploring the ontological underpinnings of contemporary EU cybersecurity policy.

As I will elaborate in subsequent chapters, the EU's cyber policy development has taken place within the context of several internal and external crises, global power shifts, and increasing European integration in the area of foreign and security policy. These developments provide important context to examine both persistent continuities within the EU's cybersecurity outlook and significant changes. To foreground the influence of this context, I first advocate for a more explicit focus upon the ontological basis of cybersecurity policy.

Chapter II - Review of the Literature

This chapter reviews the literature which comprises the basis for approaching the question of how geopolitical and sovereigntist language has emerged in the EU's cybersecurity policy. Extant international relations (IR) and political science scholarship has established—albeit equivocally—that cyberspace presents significant ontological challenges with which policymakers must grapple as they develop cyber policies and strategies. In mainstream literature, scholars have tended to explain actors' strategic behaviour as being conditioned by particular material or state-based capabilities, taking for granted the ontological assumptions which make such capabilities 'matter' in the first instance. At the same time, the state-centric and realist ontological assumptions underlying these explanations cannot adequately grasp EU policy dynamics in the cybersecurity context.

To remedy these shortcomings, this chapter subsequently turns to the smaller body of constructivist and ideational scholarship on the topic, which offers a promising approach for exploring the emergence of geopolitical and sovereigntist language in EU policy discourse. It advocates for an explicit focus upon the ontological dimension to cyber policy and concludes with the benefits of undertaking such an approach.

Cyber Policymaking Challenges

Political science and IR scholarship has equivocated that the cyber policy domain is rife with ontological challenges. While the 'ontological dimension' to this literature is often implicit, it has nonetheless demonstrated that policymakers struggle with several fundamental features of cyberspace: its conceptualization, the scope of cyber threats and insecurities, and *states'* existential survival in such an environment.

The ontological challenge posed by cyberspace — be it as an environment, policy domain, or an object of analytic inquiry—is underscored by the fact that its definition remains subject to intense debate.[1] Political science literature has generally remained atheoretical, thus evading direct confrontation with the ontological underpinnings of cyberspace; 'deferring substance' in the words of Hedvig Ördén[2] to focus upon programmatic and institutional challenges faced by actors towards cyberspace.[3] Underlying the baseline consensus that cyberspace is a complex, multi-layered environment[4] remain conceptual gaps and contradictions regarding its fundamental features, such as the number, substance and type of 'layers' of cyberspace.[5] In the discipline of IR, scholars have called for further theoretical innovation beyond the 'traditional Westphalian mould', given that cyberspace challenges classical understandings of statecraft, security, and international relations.[6] While such scholarship agrees that the 'cyberization of IR' has changed the rules of the game,[7] it has nevertheless shied away from confronting the theoretical implications of applying the 'old rules' to a new (cyber) game.[8]

Underlying these voracious debates lies tension between cyberspace and the 'trinitarian view' of international relations upon which the European and international security orders have

[1] However, I will be using the term 'cyberspace' as that is the term officially used by EU cyber strategies and EU documents. For contrast, refer to Lucas Kello, *The Virtual Weapon and International Order* (Yale University Press, 2017), https://doi.org/https://doi.org/10.2307/j.ctt1trkjd1, who distinguishes between cyberspace as a structural/technical environment and the cyber domain as consisting of the human (social and political) elements.

[2] Hedvig Ördén, "Deferring Substance: EU Policy and the Information Threat," *Intelligence and National Security* 34, no. 3 (2019): 421–37, https://doi.org/10.1080/02684527.2019.1553706.

[3] Myriam Dunn Cavelty, "European Politics and Society Europe's Cyber-Power Europe's Cyber-Power," *European Politics and Society*, 2018, https://doi.org/10.1080/23745118.2018.1430718.

[4] For instance, refer to Georgios I. Zekos, "Demolishing State's Sole Power over Sovereignty and Territory Via Electronic Technology and Cyberspace.," *Journal of Internet Law* 17, no. 5 (2013): 3–17, http://proxy.lib.sfu.ca/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=91743838&site=ehost-live; M. Blumenthal and D. D. Clark, "The Future of the Internet and Cyberpower.," in *Cyberpower and National Security*, ed. F.D. Kramer, S. Starr, and L.K. Wentz (Washington: National Defense University Press, 2009); Martin C. Libicki, *Conquest in Cyberspace* (Cambridge: Cambridge University Press, 2007); Dunn Cavelty, "European Politics and Society Europe's Cyber-Power Europe's Cyber-Power."

[5] Nazli Choucri and David D. Clark, "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma," in *Explorations in Cyber-International Relations: Who Controls Cyberspace?* (Cambridge: MIT Press, 2012); Libicki, *Conquest in Cyberspace*.

[6] Kello, *The Virtual Weapon and International Order*; Dunn Cavelty, "European Politics and Society Europe's Cyber-Power Europe's Cyber-Power."

[7] Melania-Gabriela Ciot, "Cyberspace and the New World Order," *Studia Universitatis Babeș-Bolyai Studia Europaea* 62, no. 2 (2014): 5–15.

[8] Albeit with some exceptions: Dunn Cavelty, "European Politics and Society Europe's Cyber-Power Europe's Cyber-Power"; Lucas Kello, "The Quest for Cyber Theory," in *The Virtual Weapon and International Order* (Yale University Press, 2017), 23–57, https://doi.org/10.2307/j.ctt1trkjd1.6; Blumenthal and Clark, "The Future of the Internet and Cyberpower."; Jan-Frederik Kremer and Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges* (New York: Springer Press, 2014), https://www.springer.com/gp/book/9783642374807.

been historically based. The 'trinitarian view' of international relations conceives of the state, sovereignty, and military as territorially packaged into 'a bordered power container.'[9] Sovereignty is therefore constituted by a Westphalian 'state-force-territory relation.'[10] Indeed, this conception inspired John Agnew's famous argument about the 'territorial trap', in which 'geographical division of the world into mutually exclusive territorial states […] has served to define the field of study.'[11] By contrast, cyberspace encompasses weak locational factors, networked hierarchies in which power is diffused rather than transferred and greater access for non-state actors to exert power.[12] Thus having a more fluid, complex, and tenuous link with 'Westphalian geography', cyberspace tends to 'represent a threat to the spatialized forms of intelligibility and control'[13] by challenging the 'Westphalian' contiguity between (nation-state) sovereign authority.[14]

Despite these tensions, states have resolved to ensure control and security in cyberspace.[15] The current trend towards the 'Balkanization of the internet' and cyber- 'spheres of influence' reflects this dynamic as well as the broader context of a power shift in international relations: the rise of China.[16] Thus, as Myriam Dunn Cavelty and Thierry Balzacq have argued, cyberspace cannot be essentialized into a post-Westphalian geographical space or as a 'clean break' from Westphalian traditional actors and institutions.[17]

---

[9] Anthony Giddens, *The Nation State and Violence: Volume Two of A Contemporary Critique of Historical Materialism* (Cambridge: Polity, 1985).

[10] Tarak Barkawi, "Decolonising War," *European Journal of International Security* 1, no. 2 (2016): 199–214, https://doi.org/10.1017/eis.2016.7; See also: Stephen D. Krasner, "Compromising Westphalia," vol. 20, 1995, https://about.jstor.org/terms.

[11] John Agnew, "The Territorial Trap: The Geographical Assumptions of International Relations," *Review of International Political Economy* 1, no. 1 (1994): 53.

[12] Mariarosaria Taddeo, "Cyber Conflicts and Political Power in Information Societies," *Minds and Machines* 27, no. 2 (2017): 265–68, https://doi.org/10.1007/s11023-017-9436-3; Joseph S Nye Jr, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2017): 44–71, https://doi.org/10.1162/ISEC_a_00266.

[13] Thierry Balzacq and Myriam Dunn Cavelty, "A Theory of Actor-Network for Cyber-Security," *European Journal of International Security* 1, no. 2 (2016): 186, https://doi.org/10.1017/eis.2016.8.

[14] Seán Patrick Eudaily and Steve Smith, "Sovereign Geopolitics? Uncovering the 'Sovereignty Paradox,'" *Geopolitics* 13, no. 2 (2008): 309–34, https://doi.org/10.1080/14650040801991621; Burak Kadercan, "Triangulating Territory: A Case for Pragmatic Interaction between Political Science, Political Geography, and Critical IR," *International Theory* 7, no. 1 (2015): 125–61, https://doi.org/10.1017/S1752971914000402.

[15] Joseph S. Nye Jr., "The Regime Complex for Managing Global Cyber Activities," *CIGI Publications*, no. 1 (2014): 1–15..

[16] James A. Lewis, "Sovereignty and the Evolution of Internet Ideology," *CSIS*, 2020, https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology; Weber, "Making Sense of Technological Spheres of Influence."

[17] Balzacq and Dunn Cavelty, "A Theory of Actor-Network for Cyber-Security."

Perhaps as a consequence of this tension, a plethora of scholarship has equivocated that traditional state security providers contend with *ontological* anxieties in their efforts to provide cybersecurity. [18] Whereas Joseph Nye Jr. stressed the ambiguity of international law in the case of cyber threats and the threshold of force,[19] Tomasz Aleksandrowicz (2015) argued that states have been forced to operate in a 'legal vacuum' and at higher levels of risk due to the lack of basic international rules on cyberspace.[20] Alternately, Erik Gartzke and Jon Lindsay distinguished between the *possibility* of harm through cyberspace and the *probability* of harm (whereby the latter is determined by human agents).[21] Their argument, in agreement with Thomas Rid,[22] implies that the level of anxiety about cyberspace might be unrepresentative of the *actual* level of harm it poses to actors.

While advancing an opposing perspective about the harmful potential of virtual weapons, Lucas Kello highlighted another ontologically disruptive implication of cyberspace: that it blurs the concepts of 'war' and 'peace'—the two primary constituent units which underpin the 'nature' of international relations. [23] Maria Mälksoo agrees, arguing that cybersecurity challenges expose 'collective actors to the fundamental existential questions about the continuity of their external environment as they know it' as well as their own existential vulnerability 'to unknown and indeterminate threats.'[24] As a consequence, cyber warfare, like hybrid warfare, is highly unsettling to actors' ontological understanding of how

[18] Ronald J. Deibert and Rafal Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security," *International Political Sociology* 4, no. 1 (March 1, 2010): 15–32, https://doi.org/10.1111/j.1749-5687.2009.00088.x; Jon Lindsay et al., "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," 2016; Clement Guitton, "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?," *European Security* 22, no. 1 (2013): 21–35, https://doi.org/10.1080/09662839.2012.749864.

[19] Nye Jr., "Deterrence and Dissuasion in Cyberspace."

[20] Tomasz R. Aleksandrowicz, "Cyberspace as a Source of Threat to National Security. An Attempt to Conceptualize the Problem," *Internal Security* 7, no. 1 (2015): 187–204, https://doi.org/10.5604/20805268.1192777.

[21] Lindsay et al., "Coercion through Cyberspace: The Stability-Instability Paradox Revisited."

[22] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 5–32, https://doi.org/10.1080/01402390.2011.608939.

[23] Lucas Kello, "Technological Revolution and International Order," *The Virtual Weapon and International Order*, 2017, 80–116, https://doi.org/10.2307/j.ctt1trkjd1.8.

[24] Maria Mälksoo, "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO," *European Security* 27, no. 3 (2018): 378, https://doi.org/10.1080/09662839.2018.1497984.

the 'world works', as the circumstances under which existential threats can be expected are rendered indeterminate and unpredictable. [25]

Within this broader context, scholars such as Helena Carrapico and Benjamin Farrand have demonstrated that the EU has struggled to conceptualize cyberspace as a strategic domain,[26] suggesting that EU policymakers indeed experience ontological challenges. Beyond this observation, however, the relationship between the EU's ontological assumptions about cyberspace, the substantive content of its policies, and its conceived role as a cyber actor has not been explored to a significant extent. In this conversation, scholars have argued that the EU is further affected by institutional challenges, particularly the diffusion of external relations governance across several EU institutional areas, which have stymied the EU's cybersecurity policy coherence.[27] This insight is not specific to the cyber policy domain, however; it echoes scholarly criticisms of the EU's activities in other foreign policy areas, such as its external relations with third countries.[28] It reflects the structural fragmentation of its external relations policy, which precludes 'natural synergies' horizontally (between EU institutions) and vertically (between the EU and member states) and reduces the EU's capacity to speak with one voice.[29] Accordingly, work on incoherence alone cannot explain how EU policymakers conceive of the *unique challenges* which cyberspace presents.

---

[25] Hybrid warfare tears apart the tidy war/peace binary that characterizes conventional warfare, blurring the boundaries between civilian and military through operating in the 'gray'. At the same time, it blurs the 'external' and 'internal' dimensions of policymaking to a degree that unsettles the typical foreign/domestic policy divide. See for example Mälksoo (note 23); or Claudia Major and Christian Mölling, "A Hybrid Security Policy for Europe. Resilience, Deterrence, and Defense as Leitmotifs," 2015.

[26] Dunn Cavelty, "European Politics and Society Europe's Cyber-Power Europe's Cyber-Power"; Helena Carrapico and André Barrinha, "The EU as a Coherent (Cyber)Security Actor?," *Journal of Common Market Studies* 55, no. 6 (2017): 1254–72, https://doi.org/10.1111/jcms.12575; Elaine Fahey, "The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security" (Amsterdam, 2014).

[27] Annegret Bendiek, Raphael Bossong, and Matthias Schulze, "The EU's Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges," 2017; Carrapico and Barrinha, "The EU as a Coherent (Cyber)Security Actor?"; Fahey, "The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security."

[28] See for example Maurizio Carbone, "The European Union and China's Rise in Africa: Competing Visions, External Coherence and Trilateral Cooperation," *Cooperation and Conflict* 29 (2011): 203–21, https://doi.org/10.1080/02589001.2011.555195; Karolina Pomorska and Sophie Vanhoonacker, "Europe as a Global Actor: Searching for a New Strategic Approach," *Journal of Common Market Studies* 54, no. April (2016): 204–17, https://doi.org/10.1111/jcms.12430; Arne Niemann, Charlotte Bretherton, and Johannes Gutenberg, "EU External Policy at the Crossroads: The Challenge of Actorness and Effectiveness," *International Relations* 27, no. 3 (2013): 261–75, https://doi.org/10.1177/0047117813497306.

[29] Reuben Wong and Christopher Hill, "National and European Foreign Policies: Towards Europeanization," *National and European Foreign Policies: Towards Europeanization*, no. April (2012): 1–280, https://doi.org/10.4324/9780203816035.

The dearth of EU studies examining the ontological dimension to EU cyber policy—particularly how policymakers conceive of cyberspace in an EU context—is a notable gap, given that the EU continually navigates the 'trinitarian' view to international relations and questions of sovereignty throughout the unfolding process of European integration. By virtue of its supranational structure, multilateral decision-making processes and a political culture geared towards transborder, horizontal integration,[30] the EU's experience arguably presents an alternative for contending with the entanglement of Westphalian and post-Westphalian elements of the cyber domain. Similar to cyberspace, European integration has been referred to as a process of 'boundary re-definition' which requires national *disintegration* of state boundaries.[31] Thus, the EU's relationship with boundaries and territoriality is atypical to the Westphalian model; unlike nation-states, the EU does not have the capacity to operate 'with more or less the same boundary around its functional tasks.'[32] Yet, the EU has not made a full-fledged departure from the nation-state, particularly in terms of where it derives sovereign authority.[33] The insights of European integration studies therefore call for a deeper exploration of how the EU's institutional experience interplays with the broader ontological dimension of cyberspace—beyond the concept of 'incoherence'—and its engagement with geopolitical and sovereigntist language.

Overall, scholarship has recognized the ontological challenge posed by cyberspace, including in the EU policy context. However, it has not examined in-depth how the EU has responded to these challenges, nor its potential link to the EU's expression of geopolitical language. As I explore below, the literature focusing upon policy responses is overly materialist

[30] George Christou, "The EU's Approach to Cyber-Security," EU Commission Lifelong Learning Programme, 2017.

[31] Hans Vollaard, *European Disintegration : A Search for Explanations* (New York: Palgrave MacMillan, 2018); Bruno Zanon, "Infrastructure Network Development, Re-Territorialization Processes and Multilevel Territorial Governance: A Case Study in Northern Italy," *Planning Practice and Research* 26, no. 3 (2011), https://doi.org/10.1080/02697459.2011.580114.

[32] Stefano Bartolini, *Restructuring Europe: Centre Formation, System Building, and Political Structuring between the Nation State and the European Union*, Online (Oxford: Oxford Scholarship Online, 2006), https://doi.org/10.1093/0199286434.001.0001.

[33] John Erik Fossum, "Conceptualizing the European Union Through Four Strategies of Comparison," *Comparative European Politics* 4 (2006): 94–123, https://doi.org/10.1057/palgrave.cep.6110077.

in orientation, and its state-centric, realist disposition has encouraged particular assumptions about the EU as a cyber actor.

Acting Upon Ontologies

Notably, IR and political science scholarship has devoted relatively scarce attention to the relationship between EU cyber policy and geopolitics in cyberspace. Despite scholarly recognition that the EU's strategic posture in cyberspace has a 'geopolitical dimension', these claims have only been made in passing.[34] Beyond this cursorial acknowledgement, the distinctive meaning and presence of 'geopolitics' in the EU cyber policy context has not been examined to a significant extent, let alone the question of sovereignty. Nonetheless, the wider literature on cyberspace, specifically strategic studies, security studies, and IR, has more extensively explored the link between geopolitics and cybersecurity. As I detail in this section, this scholarship has primarily argued that hard power capabilities, material resources (particularly technological superiority), and intelligence prowess comprise the main determinants for an actor's policy behaviour.

In mainstream literature, scholars such as Jon Lindsay and Erik Gartzke have generally emphasized the significance of cyberwarfare capabilities and a strong intelligence arm for strategizing in global cyberspace.[35] Other 'hard power' resources, including control over critical technologies, are also viewed as key factors for decision-making. While exceptions exist,[36] the conventional approach to 'cyber capabilities' is to adopt a state-centric orientation[37]

[34] Annegret Bendiek and Eva Pander Maat, "The EU's Regulatory Approach to Cybersecurity," 2019; Thomas Renard, "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain," *European Politics and Society* 19, no. 3 (2018): 321–37, https://doi.org/10.1080/23745118.2018.1430720; Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *Philosophy and Technology* 33, no. 3 (2020): 369–78, https://doi.org/10.1007/s13347-020-00423-6; Łukasz Antoni Król, "Digital Foreign Policy: How Digital Tools Can Further Europe's Foreign Policy Goals," *European View* 15, no. 1 (2016): 133–44, https://doi.org/10.1007/s12290-016-0384-8; Julia Pohle and Thorsten Thiel, "Digital Sovereignty," *Internet Policy Review* 9, no. 4 (2020): 1–19, https://doi.org/10.14763/2020.4.1532.

[35] Cuhong Cai, "Geopolitics in the Cyberspace: A New Perspective on U.S.-China Relations.," *The Journal of International Studies* 39, no. 1 (2018), http://jtp.cnki.net/bilingual/detail/html/GJZY201801001?view=3; Lindsay et al., "Coercion through Cyberspace: The Stability-Instability Paradox Revisited"; Lewis, "Sovereignty and the Evolution of Internet Ideology"; Frédérick Douzet, "Understanding Cyberspace with Geopolitics," *Hérodote* 1, no. 152–153 (2014): 3–21, https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm.

[36] Including within 'critical approaches' to strategic and security studies (Liebetrau and Christensen, 2020; Ördén, 2019).

[37] Including Dmitry Brizhinev, Nathan Ryan, and Roger Bradbury, "Modelling Hegemonic Power Transition in Cyberspace," *Complexity* 2018 (2018), https://doi.org/10.1155/2018/9306128; Sean Lawson, "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats," *Journal of Information Technology and Politics* 10, no. 1 (January 2013): 86–103,

and to draw upon realist paradigmatic assumptions (in accordance with classical IR theory),[38] as exemplified by Gartzke and Lindsay. These assumptions implicate how geopolitical dynamics are understood in cyberspace by scholars and practitioners, and thus influence how policymakers formulate strategies with such dynamics in mind.

Realists broadly subscribe to the notion of 'power-politics', assuming that the state is a unitary, rational actor in an anarchical international environment.[39] In such a Hobbesian-like international system, possessing hard-power capabilities (e.g. intelligence and military strength) and material resources are crucial for states to engage in 'self-help' strategies and power-balancing.[40] Material and territorial resources are held to form the basis of cyber capabilities; realist game-theoretic approaches, such as James Fearon's recent work, have measured cyber capabilities in terms of a *state's* capacity to *seize territory* in cyberspace.[41] Conceptually, geopolitics in cyberspace is approached by realists as a competition over 'power and interests through controlling space,' in which there is a balance-of-power struggle between states, in a matter adherent to the trinitarian conception of international security.[42] The popular conception of cyberspace as a power-politics struggle between the US and China draws upon this paradigm.

To explain EU cyber policy responses, scholars have chiefly drawn upon *intergovernmentalist* theory, which may be situated within the realist paradigm.[43]

---

https://doi.org/10.1080/19331681.2012.759059; Erik Gartzke and Jon R Lindsay, "Security Studies Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," 2015, https://doi.org/10.1080/09636412.2015.1038188; Rid, "Cyber War Will Not Take Place"; Stuart H Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, 2009; D. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, ed. F. D. Kramer, S. H. Starr, and L.K. Wentz (Washington, DC: National Defense University Press, 2009).

[38] Dunn Cavelty, "European Politics and Society Europe's Cyber-Power Europe's Cyber-Power."

[39] Hans J. Morgenthau, *Politics Among Nations : The Struggle for Power and Peace*, 4th ed. (New York NY: Alfred A. Knopf, 1948).

[40] Jolyon Howorth and Anand Menon, "Still Not Pushing Back: Why the European Union Is Not Balancing the United States," *Source: The Journal of Conflict Resolution* 53, no. 5 (2009): 727–44, https://doi.org/10.1177/0022002709339362; Morgenthau, *Politics Among Nations : The Struggle for Power and Peace*; Stephen M. Walt, "The Renaissance of Security Studies," *International Studies Quarterly,* 35, no. 2 (1991): 211, https://doi.org/10.2307/2600471.

[41] James D. Fearon, "Cooperation, Conflict, and the Costs of Anarchy," *International Organization* 72, no. 3 (2018): 523–59, https://doi.org/10.1017/S0020818318000309.

[42] Merje Kuus, "Policy and Geopolitics: Bounding Europe in EUrope," *Annals of the Association of American Geographers* 101, no. 5 (2011): 1140–55, https://doi.org/10.1080/00045608.2011.577362.

[43] Simon Hix, "The Study of the European Community: The Challenge to Comparative Politics," *West European Politics,* 17, no. 1 (1994): 1–30, https://doi.org/10.1080/01402389408424999.

Intergovernmentalism holds that national governments retain control over foreign policy and defence; thus, further European integration (as *intergovernmental* cooperation) is determined by the interests of Member States.[44] According to this theorization, the EU's policy development is the reflection of Member States' pooled sovereignty and diverse national interests.[45] Adopting this approach, Krzysztof Feliks Sliwinski's (2014) study holds that pooled sovereignty constrains the EU's capacity to develop an assertive role for itself as a cybersecurity actor due to inconsistencies between national security narratives.[46] He contends that 'traditional sovereignty claims are more than likely to leave the EU toothless in the future.'[47] Sliwinski's explanation therefore does not anticipate the EU's invocation of *European sovereignty* in its most recent strategy, if, as he argues, the conflicting 'traditional' sovereignty claims of Member States will constrain the EU's capacity to imagine a role in cyberspace beyond that of a 'facilitator'. Yet, his contribution suggests there is a possibility that *Member State preferences* could be driving the EU's strategic shift towards 'European sovereignty'.

Nevertheless, a state-centric, intergovernmentalist focus cannot provide a full account of the emergence of EU-specific norms and interests in the EU's cyber strategy, such as its aspiration for 'European sovereignty' in cyberspace. At the fundamental level, it is evident that the EU is not a nation-state actor in the conventional sense of the term.[48] As Sjursen evinces, EU foreign and security policy 'is shaped with reference to values and principles that are seen as *particular* to the Union, and not with exclusive reference to the interests and values of the member states.'[49] This is laid bare by the fact that, at the time of the release of the first EU-

[44] Stanley Hoffmann, "Obstinate or Obsolete ? The Fate of the Nation-State and the Case of Western Europe," *Daedalus* 95, no. 3 (1996): 862–915.

[45] Hoffmann.

[46] Sliwinski, "Moving beyond the European Union's Weakness as a Cyber-Security Agent."

[47] Sliwinski, 470.

[48] Fossum, "Conceptualizing the European Union Through Four Strategies of Comparison"; Magali Gravier, "Empire vs Federation: Which Path for Europe?," *Journal of Political Power* 4, no. 3 (2011): 413–31, https://doi.org/10.1080/2158379X.2011.628854.

[49] Helene Sjursen, "Not so Intergovernmental after All? On Democracy and Integration in European Foreign and Security Policy," *Journal of European Public Policy* 18, no. 8 (2011): 1089, https://doi.org/10.1080/13501763.2011.615194.

level cyber strategy (in 2013), over half of EU Member States did not have national-level cyber strategies, nor clear preferences regarding security in cyberspace.[50] To this end, the EU-wide cybersecurity directive has served as the 'vehicle for shaping policies and cyber-capacities at both the EU and the Member State level.'[51] This contravenes the intergovernmentalist assumption that national governments are the primary drivers of EU-level cybersecurity policy.

Furthermore, materialist, capabilities-oriented and state-centric approaches fail to account for the EU's capabilities-expectations gap, which refers to the persistent disconnect between the EU's capabilities and its rhetoric in the area of common foreign and security policy.[52] Annegret Bendiek and colleagues' analysis of Council decisions from 2009-2020 reveals the presence of such a gap, in which the number of Council press releases (often produced in the absence of reaching a common EU position) has risen, despite the consistent decline in EU common foreign and security policy (CFSP) outcomes over time (*refer to Appendix 1*).[53] The clear presence of a 'capabilities-expectations' gap underlines that greater attention should be paid to the EU's discourse. The sole focus on CFSP policy outcomes cannot capture the thematic areas of disagreement or debate between Member States (given that contentious issues are absent in CFSP decisions). However, these debates may nevertheless influence the EU's self-representation in cyberspace, and should be subject to scrutiny.

Moreover, scholars have deemed state-centric studies inadequate for fully capturing the multifaceted reality of cybersecurity practices.[54] As Tobias Liebetrau and Kristoffer Kjærgaard Christensen contend, 'much of the politics of cyber security play out among actors and in sites

[50] Patryk. Pawlak et al., *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building*, 2018, https://doi.org/10.2815/38445.

[51] Panagiotis Trimintzios et al., "Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU" (Brussels, 2017).

[52] Coined by Christopher Hill in 1993, 'capabilities' refers to conventional policy instruments, resources, and coherence ('the ability to take decisions and hold to them'). Expectations refers to 'those ambitions or demands of the EU's international behaviour which derive from both inside and outside the Union'. In Annegret Bendiek, Minna Ålander, and Paul Bochtler, "CFSP: The Capability-Expectation Gap Revisited. A Data-Based Analysis," 2020, 6, https://www.swp-berlin.org/fileadmin/.

[53] Bendiek, Ålander, and Bochtler.

[54] The rival to realist approaches, critical security studies, has also been criticized for solely focusing upon the national context, situating cybersecurity within the confines of the 'national' and centering the role of *national* security actors in their analyses. In Liebetrau and Christensen, "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites and Spaces."

and spaces of security politics that evade traditional forms of national security' due to the interconnected, diffuse, and ever-evolving nature of digital technologies.[55] Therefore, a state-centric approach may not afford due consideration to the role of EU-level (or supranational) drivers in shaping the EU's cyber policy development.

Overall, a great deal of work reproduces particular ontological assumptions about geopolitical/strategic and security dynamics in cyberspace (and thus the scope and nature of policy responses). Through reviewing this literature, it can therefore be seen how the application of ontological assumptions associated with the realist paradigm to cyberspace—namely the key role of the state, hard-power capabilities, and the trinitarian view of international relations—have also shaped *scholarly* analyses of cyberspace. Given that such work inadequately grapples with EU cybersecurity policy dynamics, it is worthwhile to turn to scholarship that suggests that ideational factors, in addition to those highlighted in mainstream scholarship, play a vital role in shaping the trajectory and substance of the EU's cyber policy.

Expressing Ontologies

By foregrounding the link between ideas and policy behaviour, ideational and interpretive scholarship has the analytical tools to uncover the linkage between an actors' ontological approach and their policy response. Valuably, this literature has demonstrated that policymakers draw upon existing spatial notions of power and security to legitimize their use of particular policy instruments. However, it has yet to thoroughly consider this insight in the EU cybersecurity context.

Securitization is perhaps the most prominently featured concept in IR literature about discursive dynamics in cyberspace.[56] It is classically understood as political elites' discursive

[55] Liebetrau and Christensen, 6.
[56] Balzacq and Dunn Cavelty, "A Theory of Actor-Network for Cyber-Security."

construction of particular objects as existential threats to survival through a 'speech act'.[57] Scholars such as George Christou (2016, 2019), Carrapico and Farrand (2020) have traced how securitization has risen to primacy within EU policy discourses; others have demonstrated its presence within state actors.[58] This discursive trend is widely held to be a response to proliferation of state-sponsored cyberattacks over the last two decades, and the widespread perception that cyberspace provides an accessible and ambiguous means to conduct warfare.[59]

More recently, discourse-oriented work has identified a second trend: the invocation of geopolitical, sovereigntist, and spatial metaphors to legitimize the extension of state and/or regulatory control into cyberspace. This global shift was characterized by a move from purely technical and securitized narratives towards geopolitical and sovereigntist assertions. Policymakers have leveraged metaphors such as the 'Digital Cold War'[60] as a heuristic device to approach the complexity of cyberspace, although such analogies have been deemed as inadequate representations of cyberspace.[61] However, empirical explorations about this trend have generally excluded the EU context, which has led to a notable gap in this body of literature. Temporal limitations could partially explain this omission, given that the EU's overt engagement with geopolitical and sovereigntist language has only emerged (approximately) over the last three years. Nonetheless, it was notably absent in Carrapico and Farrand's (2020) analysis on EU cyber policy discourses, which found that the EU has shifted towards deprioritizing the role of public-private partnerships in its cybersecurity strategy over time.[62]

---

[57] Barry Buzan and Ole Wæver, *Regions and Powers: The Structure of International Security* (Cambridge: Cambridge University Press, 2003).

[58] George Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, ed. Stuart Croft, *New Security Challenges Series* (Hampshire: Palgrave MacMillan, 2016), https://doi.org/10.1080/09662839.2016.1160892; George Christou, "The Collective Securitisation of Cyberspace in the European Union," *West European Politics* 42, no. 2 (February 23, 2019): 278–301, https://doi.org/10.1080/01402382.2018.1510195; Helena Carrapico and Benjamin Farrand, "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy," *Journal of European Integration* 42, no. 8 (2020): 1111–26, https://doi.org/10.1080/07036337.2020.1853122; Luísa Cruz Lobato and Kai Michael Kenkel, "Discourses of Cyberspace Securitization in Brazil and in the United States," *Rev. Bras. Polít. Int* 58, no. 2 (2015): 23–43, https://doi.org/10.1590/0034-7329201500202.

[59] Cruz Lobato and Michael Kenkel, "Discourses of Cyberspace Securitization in Brazil and in the United States."

[60] Lewis, "Sovereignty and the Evolution of Internet Ideology"; Joshua Rovner and Tyler Moore, "Does the Internet Need a Hegemon?," *Journal of Global Security Studies* 2, no. 3 (July 1, 2017): 184–203, https://doi.org/10.1093/jogss/ogx008; David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue* 44, no. 2 (2013): 147–64, https://doi.org/10.1177/0967010613478323; "The Tech Cold War Between the U.S. and China Is Heating Up," The New York Times, 2020, https://www.nytimes.com/2020/10/01/business/dealbook/tech-cold-war-us-china.html.

[61] Betz and Stevens, "Analogical Reasoning and Cyber Security."

[62] Carrapico and Farrand, "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy."

Surprisingly, their study did not consider whether this ideational shift was related to the EU's prominent emphasis on digital sovereignty, nor the EU's recent geopolitical and security concerns about Chinese state-backed private companies (e.g. Huawei) in the EU's Digital Single Market.

Elsewhere, the interplay between geopolitics, cybersecurity discourse, and actors' orientations towards sovereignty have been of increasing interest. For one, Julia Pohle and Thorsten Thiel identified a significant trend in the application of sovereignty to cyberspace: as opposed to operating as a legal and organizational concept as was the traditional norm, 'digital sovereignty' has instead emerged as a *discursive practice*, premised upon two dominant ways of thinking about cyberspace, which they delineated as 'cyber exceptionalism' and 'internet governance.' [63] Whereas the former conception assumes that the rise of the internet and rapid, accessible, and networked communication has led to the erosion of state sovereignty, the latter encompasses the multistakeholder model, wherein states have 'different and non-sovereign roles' as regulators in collaboration with other stakeholders. [64] In the European context, their analysis remained fairly inconclusive: while they found that digital sovereignty discourses are generally value-driven, regulatory, and oriented towards 'a secure digital sphere', they stressed that digital sovereignty is 'not an end in itself' as it has been portrayed by European policy actors.

Overall, while discursive approaches suggest a link between securitization, the use of spatial analogies, and sovereignty discourses, no holistic explanations exist to explain the EU's contemporaneous adoption of geopolitical and sovereigntist language.

[63] Pohle and Thiel, "Digital Sovereignty."
[64] Pohle and Thiel, "Digital Sovereignty," 2.

Summary

Collectively, while this scholarship has revealed the myriad ways in which cyberspace is ontologically challenging for traditional global actors, it has not sufficiently examined how these tensions play out in the EU context. Given that the literature is more developed (both empirically and theoretically) from the standpoint of the nation-state, it has limited transferability for the EU policy context, and the EU's omission in such scholarship could indeed be symptomatic of the literature's realist and state-centric orientation. As a whole, scholarship has pointed to the need for a more thorough examination of the ideational and political context which has shaped the EU's cyber policy development, particularly with respect to the role of geopolitics and sovereignty in EU policy discourses. Thus, to conclude this chapter, I will explain the advantages of ontological security as a framework for analysis as the preliminary justification for this dissertation's theoretical approach.

The Ontological Dimension to Cybersecurity Policy

A policymakers' ontological understanding of cyberspace shapes their formation of baseline assumptions and claims about the environmental, technical, and structural features of cyberspace, and the political 'state of play' of cyberspace as a policy domain. Thus, an analytical focus upon the 'ontological dimension' to cyber policy foregrounds the under-explored nexus between how policymakers negotiate ontological challenges vis-a-vis cyberspace and their development of particular discourses and strategies. Thus, it has the tools to capture EU policymaking dynamics which have elided realist and state-centric paradigms, (which have generally taken this dynamic for granted).

Foremost, this approach draws attention to possibility of there being multiple different ontological conceptions of 'cyber securities'—or indeed *insecurities*—understood by actors in

different contexts.[65] This is particularly relevant in the context of EU cyber policy, which has over twenty different institutional actors.[66] As Liebetrau and Christensen put it, 'cyber securities are always in the making and hence precarious and, potentially, unstable,' and their continued relevance is established through their 'continued enactment and re-enactment in situated practices.'[67] Indeed, Guitton demonstrated in the British, German, and French cases that conceiving of cyber threats as national security issues 'fosters the idea that the threat is to the nation' and therefore fosters an 'us versus them' form of thinking—thus impacting policymaking and diplomatic proceedings.[68] This suggests that ontological challenges create particular *insecurities* for actors, which may explain how, or why, EU policymakers adopt particular language (such as geopolitical or sovereigntist) to help make sense of cyberspace.

Overall, extant scholarship has already suggested potential sources of ontological insecurity. Moreover, scholars have demonstrated that immanent EU-specific characteristics introduce doubts about its purpose or credibility as a security provider—such as its lack of traditional security capabilities (e.g. Sliwinski, 2014)[69]—and make it prone to ontological anxiety.[70] Indeed, the EU's role in guaranteeing the cyber security of its Member States remains complicated by its status as a *sui generis,* non-sovereign actor, and its lack of 'hard power' cyber capabilities (e.g. cyberwarfare and intelligence capacity).

Exploring the ontological dimension to cyberspace is therefore a promising contribution to extant scholarship, which has highlighted two key aspects of policy development—ontological challenges and strategies/responses—but not yet the underlying assumptions which shape this process. As I will argue in the next chapter, an analytical focus

[65] Liebetrau and Christensen, "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites and Spaces."
[66] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Institutional Map," 2020, https://www.enisa.europa.eu/cybersecurity-institutional-map/results.
[67] Liebetrau and Christensen, "The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites and Spaces," 8.
[68] Guitton, "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?", 26.
[69] Sliwinski, "Moving beyond the European Union's Weakness as a Cyber-Security Agent"; Christopher S Browning, "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War,'" *Political Geography* 62 (2018): 106–15, https://doi.org/10.1016/j.polgeo.2017.10.009.
[70] Jennifer Mitzen, "Anxious Community: EU as (in)Security Community," *European Security* 27, no. 3 (2018): 393–413, https://doi.org/10.1080/09662839.2018.1497985.

on ontological insecurity is critical for making sense of how geopolitical and sovereigntist language has emerged in the EU's contemporaneous policy discourse.

Chapter III – Theory and Methods

This chapter presents the theoretical framework, interpretive epistemology, and research design of this dissertation. I begin this chapter by introducing ontological insecurity as the principal analytical framework and the conceptual modifications which distinguish this dissertation's theoretical approach from extant theoretical approaches to the field of ontological *security* (OS). Next, I argue that exploring the ontological dimension to EU cybersecurity policy and its relationship to the surrounding political context makes it possible to understand how geopolitical and sovereigntist language came to predominate in the contemporaneous context. Specifically, the emergence of this language in EU official discourses, I argue, is the consequence of how EU policymakers have leveraged distinctive strategies to the EU's ontological insecurities in cyberspace over time: *temporal*, *relational*, and *spatial strategies of othering*. Whereas temporal othering initially enabled the delegitimization of geopolitics, spatial and relational othering led to the legitimization of geopolitics in EU official discourses and adoption of *European sovereignty* as a form of identification to differentiate the EU from other cyber actors. After presenting this argument, I lay out the interpretive methodology and research design, which is a qualitative analysis of EU textual sources and interviews conducted with EU policymakers.

Theoretical Approach

This dissertation focuses upon ontological *in*security as a prism through which it explains the emergence of geopolitical and sovereigntist language in EU cybersecurity policy discourses and its implications for the EU's self-conception as a cyber actor. To do so, I draw upon the innovative work of Jennifer Mitzen, Pertti Joenniemi, and Christopher Browning on

ontological *security* (OS). Ontological security entails the process of 'managing existential anxieties and uncertainties' about one's Self and surrounding environment.[1]

For the purposes of this study, I deliberately adopt an analytical focus upon ontological *insecurity*, which is held to be more analytically appropriate as opposed to *security* for the following reasons. First, ontological *security* has been criticized for its tendency to expect stasis as opposed to change in policymakers' behaviour under conditions of insecurity.[2] This expectation may be attributed to Anthony Giddens (1984), who introduced this theory to IR scholarship as a psychological explanation for the 'maintenance of security within and between states' in conditions of anarchy.[3] In Giddens' conception, a state adheres to its existing 'role-identity' to avoid the unbearable disorientation that ruptures to established identities and routines would cause. Scholars have faulted this approach for its tendency to expect the status quo and its failure to explain substantial change. Dissenting OS scholars have refuted this, arguing that ontological security does not necessarily equate to the search for *fixity* or *consistency* of identity.[4] As Mitzen puts it, 'Ontological security is never merely about "being" secure; it is fundamentally an approach through which we can better understand the coexistence of our need to both "be" and "become" over the course of our lives.'[5] Nonetheless, the literature on ontological security has been 'haunted' by the Giddensian theorization of the concept, insofar as it continues engage with the assumption of static identifications and the premise that an actor may only have one 'true' identity.[6]

---

[1] Mitzen, "Anxious Community: EU as (in)Security Community," 394.

[2] Carolijn Van Noort and Thomas Colley, "How Do Strategic Narratives Shape Policy Adoption? Responses to China's Belt and Road Initiative," *Review of International Studies* 47, no. 1 (2021): 39–63, https://doi.org/10.1017/S0260210520000388.

[3] John Cash, "Psychoanalysis, Cultures of Anarchy, and Ontological Insecurity," *International Theory* 12, no. 306–321 (2020), https://doi.org/10.1017/S1752971920000147.

[4] Christopher S Browning and Pertti Joenniemi, "Ontological Security, Self-Articulation and the Securitization of Identity," *Cooperation and Conflict* 52, no. 1 (2017): 31–47, https://doi.org/10.1177/0010836716653161; Justin Joque and Taiabul Haque, "Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity; Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity," 2020, https://doi.org/10.1145/3442167.3442170; Catarina Kinnvall and Jennifer Mitzen, "Anxiety, Fear, and Ontological Security in World Politics: Thinking with and beyond Giddens," *International Theory* 12 (2020): 240–56, https://doi.org/10.1017/S175297192000010X.

[5] Mitzen, "Anxious Community: EU as (in)Security Community," 398.

[6] Mills, (2004, 6), in Joenniemi, "Re-negotiating Europe's Identity: The European Neighbourhood Policy as a Form of Differentiation"; Browning and Joenniemi, "Ontological Security, Self-Articulation and the Securitization of Identity."

Given that the EU's formation as a political actor has been largely characterized by change as opposed to fixity of its identity, an emphasis on stasis would be inappropriate in this context. The progression of European integration has led to the EU's consequential adoption of new characteristics and competences over time,[7] most recently evidenced by the policy domain of cybersecurity. Its unique and evolving character has elicited arguments that the EU is identifiable precisely on the basis of its '*unidentifiability*.'[8] Furthermore, the evolving character of the EU's constitutive *political* identity, particularly given its absent consolidated 'European identity,'[9] has warranted its depiction as an 'anxious community' by Mitzen.[10] Therefore, this thesis seeks to move beyond the 'static' nature of Giddensian theorizations of ontological security toward a more flexible theorization, one that is open to the possibility of there being different conceptions of EU identities within its collective 'Self'.

Accordingly, this study theorizes *ontological insecurity* as the unsettling feeling of insecurity about one's Self and position in the world, relative to others in time and space. It encompasses the concept of '*unheimlich*'[11] which entails the opposite of feeling 'at home' (*heimlich)* and the sense of dread or unease that a particular existential 'secret' (such as a tension or contradiction in its self-representation) becomes exposed, triggering the actor's reputational castigation.[12] As opposed to approaching ontological insecurity as a 'brief

[7] Diez, "Speaking 'Europe': The Politics of Integration Discourse"; Thomas Diez, "Europe's Others and the Return of Geopolitics," *Cambridge Review of International Affairs* 17, no. 2 (2004): 319–35, https://doi.org/10.1080/0955757042000245924.

[8] As stated by Jacques Delors. In Roger Cohen, "Bureaucracy Over Blood," *New York Times*, February 24, 2007, https://archive.nytimes.com/www.nytimes.com/iht/2007/02/24/world/IHT-24globalist.html?pagewanted=print.

[9] Jurgen Habermas, "The European Nation State. Its Achievements and Its Limitations. On the Past and Future of Sovereignty and Citizenship," *Ratio Juris* 9 (1996), https://heinonline.org/HOL/Page?handle=hein.journals/raju9&id=125&div=12&collection=journals.

[10] Mitzen, "Anxious Community: EU as (in)Security Community."

[11] This concept is popularly embodied by Franz Kafka's novel, *The Metamorphosis ('Die Werwandlung', originally published in 1915),* in which the main protagonist wakes up as a cockroach, and must confront the existential consequences of this transformation—which have deeply unsettling effects on his relationships, his trust in his own environment, and his understanding of his Self. For an analysis of Kafka's work through the lens of ontological security, refer to Matthew T. Powell, "Bestial Representations of Otherness: Kafka's Animal Stories," *Journal of Modern Literature* 32, no. 1 (2008): 129–42, https://www.jstor.org/stable/25511795?seq=1#metadata_info_tab_contents.

[12] The etymology of unheimlich further speaks to the link between space, unconsciousness, and ontological security. On the one hand, it is derived from 'das Heim', or 'home'. One the other, it is related to the word 'das Geheimnis', which means 'secret'—therefore implying the *unheimlich* could entail the existential unease about a secret becoming unveiled in some way. In the German language, 'unheimlich' invariably carries a negative connotation. This is not to imply that ontological insecurity as a political phenomenon is invariably bad (in a normative sense); rather, the meaning relates to the feelings and emotions experienced by the *agent* subject to this insecurity.

interruption' in an actor's *consistent* Self, therefore, this dissertation understands ontological *in*security as a pervasive dynamic with which EU policymakers must negotiate.

My framework focuses upon *policy discourses* to elucidate how policymakers apprehend and negotiate with ontological insecurities in the EU cyber policy context. According to Mills, '[d]iscourse' is speech or writing seen from the point of view of the beliefs, values and categories which it embodies'; such beliefs are constitutive of the person's experience and ontological world view.[13] The particular ideas articulated (or not articulated) by policymakers, therefore, reveal the presence of ontological insecurities. *Policies* may be understood as a form of discourse; they are constitutive, reproducing or reconstructing an actor's particular identity or subjectivity.[14] Exploring EU *policy discourses* thus makes it possible to thoroughly unpack the constitutive link between the EU's articulation of geopolitical and sovereigntist concepts and the EU's construction of its role in the cyber environment.

Discursively constructing the identity (and role) of a collective actor is an intersubjective process whereby individuals must negotiate with the socio-cultural constructs within which the actor is situated.[15] John Cash argues that this construction is both a top-down and bottom-up process; narratives are constructed through individuals' 'psychological capacity and the social imaginaries and routines available in cultural fields they inhabit.'[16] An actor's Self is reflexive; actors engage in 'practices of identification' in order to locate the Self and 'capture a sense of being' in the world,[17] although 'neither fixity nor absolute non-fixity [of discursive constructions] is possible.'[18] As identities are constructed, not simply 'given', there

[13]In Loretta Sălăjan, "Ontological Security and the European Union Global Strategy," *Revista de Stiinte Politice*, no. 58 (2018): 23–33.

[14] Lene Hansen, *Security as Practice: Discourse Analysis and the Bosnian War* (London: Routledge, 2006), 19.

[15] John Cash, "To Dwell in Ambivalence: On the Promise and Dilemmas of Beck's 'the Art of Doubt'.," in *The Consequences of Global Disasters*, ed. A Elliot and E.L. Hsu (New York: Routledge, 2016), 169–181.

[16] Cash, 177-78.

[17] Browning and Joenniemi, "Ontological Security, Self-Articulation and the Securitization of Identity," 34.

[18] Ernesto Laclau and Chantal Mouffe, *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics* (London: Verso, 1985), 111.

remain alternative constructions 'against which the dominant identity notions have to be defended, and which offer the potential for change.'[19] It is in these areas of instability, or 'undecidability'[20] of discursive constructions that ontological insecurity thrives. In what follows, I present my theorized loci of insecurity.

Theorized Loci of Ontological Insecurities

I theorize that there are three identifiable loci of insecurities in EU cyber policy: *autobiographical*, *relational*, and *environmental* insecurities, as represented in Figure 1. These 'loci' have been developed on the basis of my interpretive analyses of EU cyber policy discourses (in textual documents and interviews), which found that insecurities and threat perceptions coalesced around certain anxieties related to the EU's autobiographical Self, its surrounding environment, or outsiders. My conceptualization of these loci was also informed by extant OS scholarship, which has empirically demonstrated that ontological insecurities may be autobiographical,[21] relational,[22] spatial/geographical,[23] or a combination thereof.

[19] Diez, "Europe's Others and the Return of Geopolitics," 321.
[20] Jacob Torfing, *New Theories of Discourse: Laclau, Mouffe and Žižek* (Oxford: Blackwell Publishing Ltd, 1999) 95-6, 119.
[21] Diez, "Europe's Others and the Return of Geopolitics"; Trine Flockhart, "The Problem of Change in Constructivist Theory: Ontological Security Seeking and Agent Motivation," *Review of International Studies* 42, no. 5 (2016): 799–820, https://doi.org/10.1017/S026021051600019X; Kinnvall and Mitzen, "Anxiety, Fear, and Ontological Security in World Politics: Thinking with and beyond Giddens."
[22] Cash, "Psychoanalysis, Cultures of Anarchy, and Ontological Insecurity"; Diez, "Europe's Others and the Return of Geopolitics"; Mitzen, "Anxious Community: EU as (in)Security Community."
[23] Browning, "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War'"; Diez, "Europe's Others and the Return of Geopolitics"; Mitzen, "Anxious Community: EU as (in)Security Community."

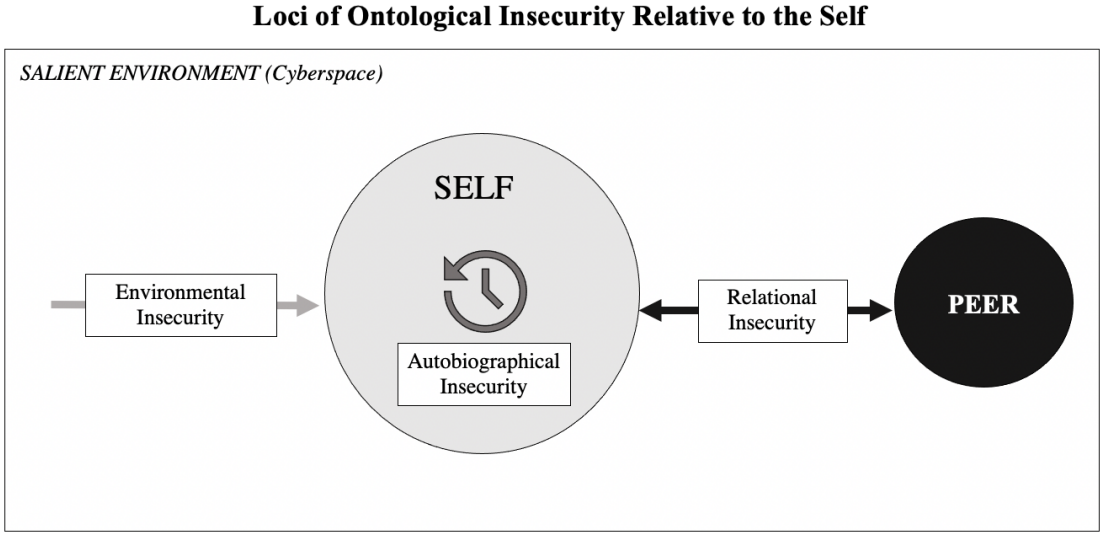


Figure 1. Various loci of ontological insecurities in EU cyber policy discourse.

Autobiographical insecurity refers to inward-looking insecurities about the 'self'—particularly regarding dislocations in one's identity *over time.* Thomaz Diez has demonstrated that the EU has historically engaged in a self-reflexive form of identity construction, in which it develops a 'loose definition' of its Self through temporal differentiation with its past.[24] However, 'dislocatory events' can undermine these identifications.[25] For a collective actor such as the EU, this includes temporal discontinuities (and/or dislocations) about how individual EU members perceive the EU's identity over time—including what role the EU should assume in a particular space, whether it is a legitimate actor, and what it should 'become.' Scholars have identified several particularly sensitive autobiographical insecurities for the EU, including portrayals of the EU as a colonizer, or as geopolitical or power-hungry actor.[26] Another example of this form of insecurity would be Euroskepticism, in which Member States question the 'point' of the EU's existence in the first instance.

Relational insecurity comprises ontological insecurity about one's Self relative to others. This includes uncertainty about what to 'expect' from others in one's surrounding

[24] Diez, "Europe's Others and the Return of Geopolitics."
[25] Diez, 321.
[26] Nicolaïdis, Kalypso, Sebe, Berny, Maas, *Echoes of Empire: Identity, Memory and Colonial Legacies*; Diez, "Europe's Others and the Return of Geopolitics"; Diez, "Speaking 'Europe': The Politics of Integration Discourse."

environment, or distrust in others' behavioural consistency. This form of insecurity may arise in contexts of confusing or unclear rules (or the lack thereof), in conditions of anarchy, or when 'the rules of the game' have changed (in IR terms). Additionally, it may emerge in circumstances when an actor is unable to acquire social recognition coherent with its self-identification. [27]

Environmental insecurity comprises ontological insecurities about the fundamental nature of the environment, thus precluding the development of a stable worldview. It is spatial insofar as it arises in contexts when there are no reliable or evident 'laws of nature', or the environment is constantly evolving in ways which threaten the actor's existence and upend existing expectations upon which their sense of 'orientation' is based.[28]

These insecurities may be experienced singularly or in concert/overlap with each other. Relational insecurities often include a spatial element, given that individuals are situated within time and space—the 'laws of nature' (environmental features) are often intimately connected to the 'rules of the game' (human constructs). However, it is worthwhile to distinguish between all of these insecurities, as they may lead to different policy responses, as demonstrated by the case of EU cyber policy.

Interplay with Securitization

Furthermore, these insecurities may interplay with another key discursive process: securitization. *Securitization* is conceptualized as an iterative, intersubjective, context-dependent and dynamic process[29] rather than solely manifested by a single speech act or event at the national level.[30] Indeed, securitization in the EU cybersecurity policy context has been an *incremental evolution* occurring through 'through the politics of routine' as opposed to a

[27] Browning and Joenniemi, "Ontological Security, Self-Articulation and the Securitization of Identity."

[28] Mälksoo, "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO"; Browning, "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War.'"

[29] Thierry Balzacq, "The Three Faces of Securitization: Political Agency, Audience and Context," *European Journal of International Relations* 11, no. 2 (2005): 171–201, https://doi.org/10.1177/1354066105052960.

[30] The latter conception is the classical conception of securitization, as theorized by Ole Wæver (2003). In Buzan and Wæver, *Regions and Powers: The Structure of International Security*.

single precipitating event outside of the realm of normal politics.[31] Securitization has implications for actors' self-conceptions as it entails 'moving away from an established sense of selfhood/subjectivity to something either more closed/exclusive or open/inclusive', a dynamic that could elicit ontological insecurity.[32] Furthermore, by aggravating perceived insecurities through the construction of particular objects or subjects as *existential* threats to survival, securitization influences how policymakers experience and express particular ontological insecurities. For one, actors are known to engage with spatial and relational concepts to securitize cyberspace,[33] which could instigate *ontological insecurities* related to the EU's positioning in the cyber environment relative to other actors. Moreover, securitization has been popularly associated with 'securitized subjectivity' which entails the construction of outsiders as 'insecure' externalities disrupting the *internal* stability of the Self.[34]

Foregrounding ontological *in*security directs analytical attention towards transformative moments when an actor's ontological security is uprooted—such as times of 'identity crises'. These 'ruptures' or 'dislocatory events' may serve as opportunities for actors to reconceptualize their own identity and their ontological understanding of the environment.[35] Given that cultural, institutional, and normative (social) routines provide an important foundation for ontological security, environmental and contextual changes can precipitate the reframing of identity.[36] During this period of 'rupture', actors may draw upon alternate identity

[31] Christou, "The Collective Securitisation of Cyberspace in the European Union," 280.
[32] Browning and Joenniemi, "Ontological Security, Self-Articulation and the Securitization of Identity." 45.
[33] For instance, a common objective for cybersecurity policy is to ensure the stability of networked *space.* As argued in Balzacq and Dunn Cavelty, "A Theory of Actor-Network for Cyber-Security."
[34] Georgios Karyotis, "European Migration Policy in the Aftermath of September 11. The Security-Migration Nexus," *Innovation: The European Journal of Social Science Research* 20, no. 1 (2007): 1–17, https://doi.org/10.1080/13511610701197783; Mitzen, "Anxious Community: EU as (in)Security Community"; Stefan Borg, *European Integration and the Problem of the State*, 1st ed. (London: Palgrave MacMillan, 2015), https://doi.org/10.1057/9781137409331.
[35] Joque and Haque, "Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity; Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity"; Kinnvall and Mitzen, "Anxiety, Fear, and Ontological Security in World Politics: Thinking with and beyond Giddens"; Bahar Rumelili, "Integrating Anxiety into International Relations Theory: Hobbes, Existentialism, and Ontological Security," *International Theory* 12 (2020): 257–72, https://doi.org/10.1017/S1752971920000093.
[36] Mitzen, "Anxious Community: EU as (in)Security Community."

representations, mobilizing cultural resources to animate *alternate* representations of identity, thus having the potential to reconfigure collective identity in the changed context.[37]

Responding to Ontological Insecurities

As ontological insecurities have the potential to seriously cripple an actor's agency, actors will seek to mitigate these *unheimlich* feelings so that they do not impede their capacity to answer 'basic existential questions' about doing, acting, and being.[38] I theorize that EU policymakers have prominently engaged in one particular type of strategy to mitigate ontological insecurities in cyberspace: '*othering*'. 'Othering' is a way of drawing boundaries around one's Self through establishing what one is *not.*[39] It is through this juxtaposition with a diametric other that an actor's identity is produced as a meaningful, legitimate and credible.[40] Othering may be negative/oppositional, neutral, or friendly; it may be used differentiate enemies *or* friends from the Self.[41] This self-construction is achieved through creating *positive* chains of association amongst discursive signifiers (self-descriptors) to construct an actor's identity and juxtaposing these signifiers with diametrically opposite, *differential* chains of association to construct the 'Other'.[42]

I delineate three forms of othering: *temporal, relational*, and *spatial*, which I argue to have characterized EU cybersecurity policy discourse and its development as a cyber actor. Table 1 lays out the theorized ontological insecurity responses that I argue to have

[37] Jelena Subotic, "Narrative, Ontological Security, and Foreign Policy Change ," *Foreign Policy Analysis* 12, no. 6 (2016), https://doi.org/10.1111/fpa.12089; Kinnvall and Mitzen, "Anxiety, Fear, and Ontological Security in World Politics: Thinking with and beyond Giddens."

[38] Catarina Kinnvall, "Globalization and Religious Nationalism: Self, Identity, and the Search for Ontological Security," *Political Psychology* 25, no. 5 (2004).

[39] Mitzen, "Anxious Community: EU as (in)Security Community."

[40] Elisabeth Johansson-Nogués, "The EU's Ontological (in) Security: Stabilising the ENP Area … and the EU-Self?," *Cooperation and Conflict* 53, no. 4 (2018): 528–44, https://doi.org/10.1177/0010836717750197.

[41] Christopher S Browning and George Christou, "The Constitutive Power of Outsiders: The European Neighbourhood Policy and the Eastern Dimension," *Political Geography* 29 (2010): 109–18, https://doi.org/10.1016/j.polgeo.2010.02.009.

[42] Hansen, *Security as Practice: Discourse Analysis and the Bosnian War*.

characterized the EU cybersecurity context, which have been identified through interpretive discursive analyses of textual sources and interviews.

Relationship to Geopolitical Language	**Locus of Ontological Insecurity**	**Mitigation Response**
Delegitimization of Geopolitics	Autobiographical	Temporal Othering
Legitimization of Geopolitics	Relational	Relational Othering
	Environmental	Spatial Othering

Table 1. Theorized ontological insecurity responses.

Whereas temporal othering engages in the *delegitimization* of geopolitics (drawing upon Mitzen's 2018 theorization), the other two responses enable its *legitimization*, building upon what Diez (2004) calls 'geopoliticized othering', which introduce the acceptability of geopolitical concepts into EU discourse. The enabling/constraining implications of each strategy for discussing 'geopolitics' create tensions and further instabilities in the EU's self-construction. Below, I address each 'othering' strategy in turn, to explore how these concepts build upon and engage with extant scholarship on the topic.

The Delegitimization of Geopolitics: Temporal Othering

Temporal othering is widely argued to be the predominant form of 'othering' with which the EU has engaged to construct its political identity and mitigate autobiographical insecurities.[43] Temporal othering is introspective and self-reflexive, focusing upon historical identifiers associated with Europe's past as the juxtaposition for the EU's current self-representation.[44] Thus, temporal othering aims to augment autobiographical insecurities about the EU's Self related to this established autobiography.[45] Scholars have argued that this othering process has provided further chronological stability and coherence to the EU's self-

[43] Diez, "Europe's Others and the Return of Geopolitics."
[44] For further reference, see Diez, "Europe's Others and the Return of Geopolitics."
[45] Mitzen, "Anxious Community: EU as (in)Security Community"; James Rogers, "From 'civilian Power' to 'Global Power': Explicating the European Union's 'grand Strategy' through the Articulation of Discourse Theory," *Journal of Common Market Studies* 47, no. 4 (2009): 831–62, https://doi.org/10.1111/j.1468-5965.2009.02007.x.

representation, which in turn has helped to bolster the EU's credibility and legitimacy as a political actor.[46]

Particularly, this strategy has been used to distinguish the EU's current Self from Europe's bloody history of Realpolitik through a particular form of temporal othering: the *delegitimization* of geopolitics.[47] As a particular form of temporal othering, *delegitimization* has served as a crucial component of the EU's 'long peace narrative', which has delegitimized policy behaviour which could be associated with the EU's violent, power-politics past. Following Mitzen (2018), delegitimization is the process of othering whereby the ideas are stigmatized but not suppressed; they are 'cognitively available but not considered socially unacceptable.'[48] In the EU's temporal self-narrative, geopolitical ideas have remained 'cognitively available' to agents—through the notion of 'never again' Realpolitik—but not socially acceptable.[49] Arguably, this form of othering does not *explicitly* thematise geopolitics, and it is not 'tied to fixed geographical borders.'[50]

Drawing upon Diez's (2004) pioneering introduction of 'geopoliticized other', my study theorizes the presence of two additional othering strategies—relational and spatial othering—which have characterized EU cyber policy and brought about the *legitimization* of geopolitical and sovereigntist language.

Relational and Spatial Othering

In 2004, Diez presciently traced a shift in the EU's discursive approach to its geographic 'Neighbourhood' to incorporate 'geopolitical othering', wherein 'identity, politics and geography are intimately linked with each other.'[51] He argues that this form of othering

[46] Flockhart, "The Problem of Change in Constructivist Theory: Ontological Security Seeking and Agent Motivation."

[47] Diez, "Europe's Others and the Return of Geopolitics"; Diez, "Speaking 'Europe': The Politics of Integration Discourse"; Mitzen, "Anxious Community: EU as (in)Security Community."

[48] Mitzen, "Anxious Community: EU as (in)Security Community," 400.

[49] Mitzen; Sonia Lucarelli and Lorenzo Fioramonti, *External Perceptions of the European Union as a Global Actor*, *External Perceptions of the European Union as a Global Actor* (Routledge Taylor & Francis Group, 2009), https://doi.org/10.4324/9780203866917.

[50] Diez, "Europe's Others and the Return of Geopolitics," 331.

[51] Diez.

constructs a particular identity group as an existential threat and locates this threat on the EU's *outside*, 'as something against which "Europe" must be defended.'[52] This conceptualization of othering can be understood as the *externalisation* of the referent subject or object. I. argue that this strategy of externalisation is a primary form of *relational othering.*

Whereas temporal othering is introspective and focused entirely on past 'Selves', *relational othering* entails the qualitative differentiation of one's own identity from outsiders (to the Self). Should actors experience *relational* ontological insecurities—that is, loss of 'basic trust' in the consistency of relationships with peers/other actors, they are compelled to engage in this strategy, which aims to buttress the actor's own self-esteem through externalising its reputational or relationship-oriented insecurities. Relational othering encompasses the OS concept of 'securitized subjectivity', in which an actor may construct its Self as a 'pure and uncomplicated being' through transposing existential anxieties about the unknown to the actor's constitutive outside (otherwise known as 'externalisation').[53] This is enacted, for example, by establishing clear 'Us versus Them' divisions, often through erecting nationalist distinctions or through bordering practices.[54]

Additionally, I delineate a second strategy—*spatial othering*—informed by Diez's (2004) insight that geopolitical othering is immanently linked to geographical space. Actors tend to engage in this strategy when they experience ontological insecurities about their position and/or existence in their surrounding environment, or 'loss of trust or uncertainty about the fundamental nature of the environment'.[55] Spatial othering, or *spatialization* is conceived as the practice of transforming one's spatial surroundings to become more compatible with the situated actor's self-positioning; to decrease one's insecurity about the environment through

[52] Diez, 332.
[53] Borg, *European Integration and the Problem of the State*.
[54] Mitzen, "Anxious Community: EU as (in)Security Community"; Subotic, "Narrative, Ontological Security, and Foreign Policy Change ."
[55] Browning, "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War.'"

establishing ‘safe spaces’. It is therefore distinctive from relational othering, as it targets the actor’s perceived security in a certain *political space* (which may not necessarily be the consequence of ‘insecure’ or ‘untrustworthy’ outsiders). In OS literature, the importance of ‘space’ for ontological security has been thematically explored with respect to the psychological significance of ‘home’ or ‘homelands’, as well as an actor’s daily self-orientation in a particular space.[56]

As distinct from relational othering, spatial othering may be *expansive* as opposed to solely externalising, as demonstrated by the significance of this strategy to the EU’s enlargement policies. Indeed, Browning (2018) argues that *spatialization* strategies seek to mitigate the EU’s ontological security within its environment through exporting the European model to its proximate environment—thus remaking the insecure environment in its own (comforting) image.[57] Scholars have described this strategy as a ‘soft form’ of geopolitics, wherein the EU pursues the development of certain geographical space in tandem with the promotion of EU values and norms.[58] In this way, the EU’s practices of spatial othering ‘seek to respond to the sense of ontological crisis surrounding EU self-conceptions, calming emerging anxieties by reaffirming a sense of self-identity, order, and stability in terms of an historically known set of coordinates.’[59]

Notably, spatial othering is often linked to relational othering due to its potential linkage with ‘outsiders’ inhabiting the environment in question. This is exemplified by the EU’s desire to create a ‘geographical ring of friends’ in its neighbourhood—by encouraging surrounding

---

[56] Jennifer Mitzen, “Feeling at Home in Europe: Migration, Ontological Security, and the Political Psychology of EU Bordering,” *Political Psychology* 39, no. 6 (2018), https://doi.org/10.1111/pops.12553; Subotic, “Narrative, Ontological Security, and Foreign Policy Change ”; Browning, “Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the ‘New Cold War.’”

[57] Browning, “Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the ‘New Cold War.’”

[58] Ian Manners, “Normative Power Europe: A Contradiction in Terms?,” *Journal of Common Market Studies* 40, no. 2 (June 1, 2002): 235–58, https://doi.org/10.1111/1468-5965.00353; Jan Zielonka, “Europe’s New Civilizing Missions: The EU’s Normative Power Discourse,” *Journal of Political Ideologies* 18, no. 1 (February 2013): 35–55, https://doi.org/10.1080/13569317.2013.750172; Thomas Diez, “Normative Power as Hegemony,” *Cooperation and Conflict* 48, no. 2 (2013): 194–210, https://doi.org/10.1177/0010836713485387; Cristian Nitoiu and Monika Sus, “Introduction: The Rise of Geopolitics in the EU’s Approach in Its Eastern Neighbourhood,” *Geopolitics* 24, no. 1 (2019): 1–19, https://doi.org/10.1080/14650045.2019.1544396.

[59] Browning, “Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the ‘New Cold War’”, 107.

countries to emulate the European model, the EU is able to establish a form of 'spatial comfort zone' and decrease uncertainties (and insecurities) in its external environment. Actors outside of this 'safe space' are thus subjected to relational othering (externalisation).

Unlike temporal othering, relational and spatial othering are not premised upon the delegitimization of geopolitics or the necessity of juxtaposing Europe's geopolitical past with the EU's current behaviour. Thus, these strategies permit the legitimization of geopolitical concepts into EU discourse. However, the use of relational and spatial othering does not imply that autobiographical insecurities about geopolitics have been resolved—merely that they do not *preclude* the acceptance of geopolitics in EU discourses. Rather, these three strategies of othering may come into tension with each other and exacerbate the EU's overall experience of ontological insecurity.[60]

The Legitimization of Geopolitics in EU Cyber Policy

Tracing how these three strategies became prominent at various points throughout the EU's cybersecurity policy development explains the EU's radical shift from eschewing geopolitics and sovereigntist terms during the 2000s towards embracing them in the late 2010s. EU policymakers' engagement with spatial and relational othering strategies was particularly consequential for the *legitimization* of geopolitical language in official EU cyber discourses, and the EU's adoption of 'European sovereignty'.

Initially, the securitization of cyberspace during the 2009-2013 period heralded that the cyber environment was a threat to the EU's survival, particularly with respect to its historical self-positioning as an economic and social security provider for its Internal Market. Thus, at this time, the locus of the EU's ontological insecurity was predominantly *internal* and *autobiographical,* as it was focused upon its anxieties about not fulfilling its *historical* role as

[60] As Browning explores in the case of the EU's 'geospatial' othering towards its Neighbourhood; the use of one strategy of othering can elicit insecurities about another aspect of one's Self. Browning (see note above).

an economic security provider for the Union. Accordingly, EU cyber policy discourses drew upon the tried-and-true strategy of temporal othering (delegitimization), in which geopolitical ideas were available but not *acceptable* in EU policy discourses.

Subsequently, during the 2014-mid 2017 period, EU policymakers experienced significant relational and environmental insecurities which converged—and came into tension with—its autobiographical insecurities in cyberspace. The confluence of these insecurities created a significant *rupture* to the EU's ontological understanding of its Self, its peers, and its conception of its environment, thrusting the EU into an existential crisis. EU policymakers responded to this dislocatory period by drawing upon *geopolitical* othering strategies: particularly relational othering and spatial othering. These strategies were given renewed emphasis by the EU's reconceptualized identity as a global actor (the result of ontological rupture), which envisioned a more 'joined-up', responsible, and *sovereign* role for Europe in global affairs.

This adjusted self-understanding became integrated into the EU's cybersecurity policy over the late 2017-2020 period, which in turn guided policymakers' prominent engagement with spatial and relational strategies of othering in its cyber policy. Alongside this reconceptualization, increasing environmental insecurities about cyberspace finalized the erosion of the EU's initial approach to geopolitics and paved the way for the concept's legitimization in EU cyber policy. Thus, in contrast to the 2009-2013 period—during which geopolitical ideas were available but not socially acceptable—the 2018-2020 period was characterized by the EU's decision to speak 'in geopolitical terms' in the cyber context. This marked another key turning point as geopolitics had become thinkable *and* acceptable in EU policy discourses. However, enduring cultural constraints and autobiographical insecurities influenced the EU's geopolitical vocabulary: while it could speak in geopolitical terms, it maintained a *different* identity from geopolitical actors in cyberspace.

To mitigate the destabilizing tension between the EU's autobiographical insecurity (which obliged the eschewal of geopolitics) and its environmental and relational insecurities (which impelled a geopolitical response), policymakers turned to the narrative of *European sovereignty* as a central cybersecurity policy goal. This discourse has served the purpose of differentiating the EU from other 'geopolitical competitors' in cyberspace, aiming to reconfigure its policies through a more culturally and ontologically acceptable narrative of 'sovereignty'. The EU's self-representation as the beacon of 'sovereign Europe', however, has remained vulnerable to ontological insecurities, as revealed by internal contestation between EU Member States, and Brussels' anxieties about its misrepresentation to external others.

Methodology and Research Design

My dissertation draws upon the framework of ontological insecurity to construct a contextual, historical, and ideational-focused narrative. Under scrutiny are EU policy discourses, particularly the language used by policymakers in the context of cybersecurity policy and in other relevant discursive settings. Language, as Lene Hansen argues, is 'ontologically significant', as 'it is only through the construction in language that 'things'—objects, subjects, states, living beings, and material structures—are given meaning and endowed with a particular identity.'[61] This is in line with the interpretive orientation towards the constitutive nature of language as a '[way] of world-making'.[62]

Accordingly, my study traces how the presence of geopolitical and sovereigntist language came to emerge within the EU's cybersecurity *discourses* and *practices*. As elaborated in the above section on discursive 'othering' strategies, discourses are a central component to my analysis. Often intertwined with discourses are *practices*, which are

[61] Hansen, "Security as Practice", 16.
[62] Peregrine Schwartz-Shea and Dvora Yanow, *Interpretive Design: Concepts and Processes.* (New York NY: Routledge, Taylor & Francis, 2012), 39.

necessary to strengthen the link between identity and discursive construction.[63] In the case of the EU, practices include the routine implementation of policy mechanisms (such as conditionality), standard operating procedures, or reiterations of its values.[64] These concepts reflect the interpretivist understanding of 'situated agency', which holds that 'inherited practices and social relationships influence decisions' but do not determine them.[65]

My theoretical framework elucidated three principal forms of ontological insecurity responses which have characterized the EU's cybersecurity policy development over time. As I elaborate below, my interpretive methodology enabled me to build this theory 'from the ground up' through its approach to generating data in an open and exploratory manner, and its epistemological orientation towards abductive reasoning, which obliges the researcher to begin with a tension or counter-intuitive finding and recursively examine the evidence.[66]

In order to conduct my discourse analysis, I first developed a chronology of primary source documents selected on the basis of 'research relevance' and the consultation of secondary sources. This enabled me to establish an appropriate timeframe for this study, which traces the ideational evolution(s) of 'geopolitics' and 'sovereignty' as concepts in EU cyber policy discourse over the years 2009-2020. The 2009-2020 timeframe covers political developments crucial to the EU's cyber policy development. Foremost, the enaction of the Lisbon Treaty in 2009 empowered the EU with (shared) competence in external relations, and its own political and legal personality alongside its Member States. The Lisbon Treaty therefore propelled a new era of institutional, political, and strategic development for the EU as a security actor, and for its strategic autonomy as a *sui generis* actor. Whereas EU cybersecurity policy had been primarily influenced by frameworks developed by other countries (particularly the

[63] Trine Flockhart, "'Me Tarzan – You Jane': The EU and NATO and the Reversal of Roles," *Perspectives on European Politics and Society* 12, no. 3 (2011): 263–82, https://doi.org/10.1080/15705854.2011.596306.

[64] While a discourse may itself be conceptualized as a practice, practices are nevertheless analytically distinct from discourses insofar and they may include unspoken elements. See for instance Pohle and Thiel, "Digital Sovereignty"; Hansen, *Security as Practice: Discourse Analysis and the Bosnian War*.

[65] Mark Bevir and Oliver Daddow, "Interpreting Foreign Policy: National, Comparative and Regional Studies" 29, no. 3 (2015): 280, https://doi.org/10.1177/0047117815600930.

[66] Schwartz-Shea and Yanow, *Interpretive Design: Concepts and Processes.*

US) and the Council of Europe, Lisbon helped bring about a distinctly 'European' approach.[67] Shortly thereafter, the EU's External Action Service (EEAS), the EU's diplomatic service, was established in 2010. The end point of the study, 2020, coincides with the release of the EU's most recent cyber strategy (whereupon geopolitics and sovereignty terminology became most prominent), and it is also the last year I can analyse conclusively.

This timeframe was periodized in line with transformative events which implicated EU's cybersecurity policy, and with the release of chief cybersecurity documents and strategies. The first time period, 2009-2013, encapsulates the release of the EU's first ever cybersecurity strategy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013); the second period, 2014-mid 2017, encapsulates its highly influential *Global Strategy for the European Union* (2016), up until the release of its updated cybersecurity strategy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (2017), and the final period, late 2017-2020, incorporates the EU's most recent and active cyber strategy, *The EU's Cybersecurity Strategy for the Digital Decade* (2020). Within this timeframe, I identified relevant sites of analysis through a temporalized mapping technique, which traces and situates the ideational positions of actors located in different policy settings.[68] Together with the interview data, this chronological mapping process facilitated further *exposure* to the perspectives of the multitude of agents involved in shaping and disseminating EU cybersecurity discourse.[69]

The mapping process also enabled me to establish appropriate analytical parameters for my interpretive analysis of the broad policy field of 'cybersecurity', which has expanded over time in the EU context. This dissertation focuses on two EU cybersecurity pillars in particular: *cyber defence* and its overlap with *network and information security*, although the third pillar,

[67] Christou, "The Collective Securitisation of Cyberspace in the European Union."
[68] Adele E. Clarke, Carrie Friese, and Rachel Washburn, *Situational Analysis in Practice: Mapping Research with Grounded Theory.* (New York: Routledge: Taylor and Francis, 2015).
[69] Clarke, Friese, and Washburn; Schwartz-Shea and Yanow, *Interpretive Design: Concepts and Processes.*

cybercrime, is mentioned indirectly in the context of cyber capacity building programmes. The reasons for this selection are threefold. First, two out of the three principal institutions involved in the cyber defence pillar—the EEAS and the European Commission—are the penholders for the EU's cybersecurity strategies. Indeed, all three of its cybersecurity strategies released to date were jointly authored by the Commission and the EEAS. Second, it is in the broad area of EU external relations and/or foreign and security policy that the EU's adoption of geopolitical discourse and sovereignty claims first emerged (and later came to overlap with cybersecurity policy). Thus, the pillar of cyber defence (which includes the same institutions involved in the EU's foreign and security policy formation) overlaps with the arena in which the language of interest initially emerged. Moreover, cyber defence is the pillar most closely linked to Member States' national security, which enables further exploration of the potential tensions between cybersecurity concerns at the EU level and national levels. Given the significant internal/external overlap between policy areas in cybersecurity—particularly between cyber defence and network and information security—the inclusion of the latter pillar is also warranted. In a simplified form, the principal EU agents and institutions in these pillars are represented in Figure 2 and include the EU Commission, the EEAS, the European Union Military Staff, and the European Defence Agency (*see also Appendix 2.1*). [70]

[70] Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*.

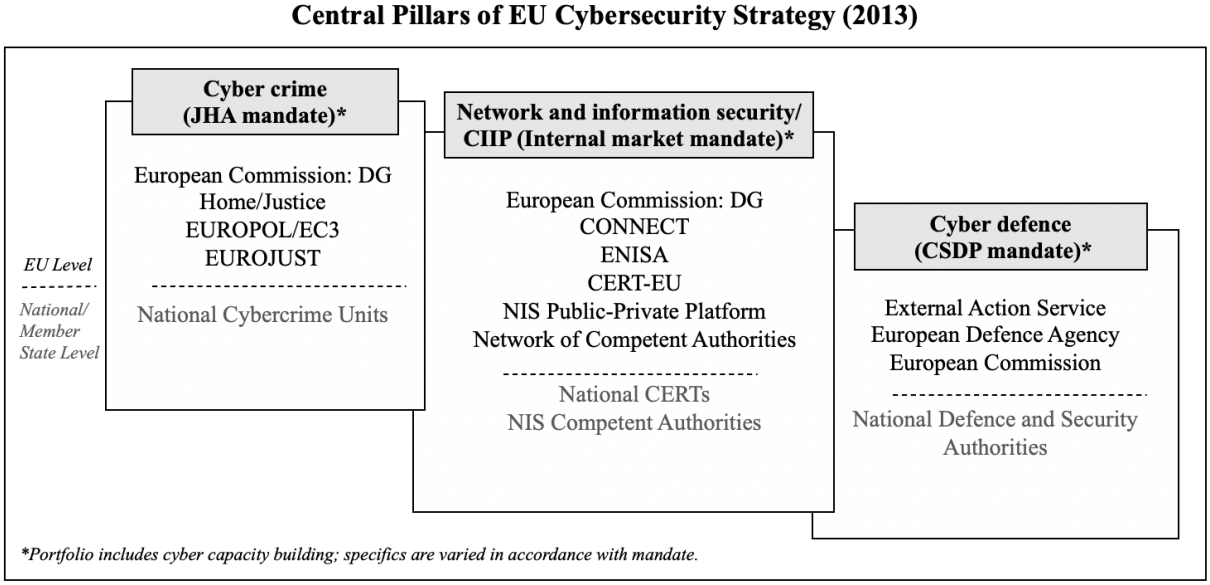


Figure 2. Central pillars of EU cybersecurity strategy (2013), as compiled by George Christou.[71] *Diagram here was reproduced, with slight modifications, by the author.*

Discourse-Analytical Method

Guided by its qualitative-interpretive research methodology, this study conducted discourse analyses of textual data and interviews in order to elucidate which beliefs and ideas underpin the concepts of geopolitics and sovereignty in the EU policy context, particularly cybersecurity and the EU external relations arenas. My approach to analysis was open and flexible, allowing meaning to emerge from the data in order to acquire a holistic understanding of the key ideas, events, and forces which have shaped the EU's cybersecurity policy development. Thus, it adhered to interpretivism's emphases on the constitutive nature of language, the crucial role of *subjectivity* and *situated-ness,* and *contingency* for knowledge formation.[72]

To recapitulate, the purpose of discourse analysis is not to reveal the objective 'truth' or the 'facts' about sovereignty or geopolitics at large, nor is it to assume that EU policymakers understand geopolitics in the same way as nation-states (or indeed scholars operating within

[71] Christou, 3.
[72] Schwartz-Shea and Yanow, *Interpretive Design: Concepts and Processes.*

particular theoretical frameworks). Rather, it is to explore the potential variation in meaning and usage of the concepts of 'geopolitics' and 'sovereignty' in the specific context of the EU's cyber policy development, and to unpack more thoroughly what ideas, events, and forces contributed to their emergence.

Document Analysis

The primary source documents analysed in this study comprise a variety of formats, including official policy documents, speeches, staff working documents, guidelines and reports, internal memoranda, transcripts of European Parliamentary debates, and discussion papers (e.g. White and Green papers). Documents were extracted from digitized archives, most frequently the EURLEX database, EU and Member State websites, and from relevant think tank and policy organizations (*refer to Appendix 4 for a list of primary textual sources)*. This dissertation also leveraged extant freedom of information requests related to EU cyber defence, including internal EU reports related to the EU Cyber Defence Policy Framework, retrieved from the AskEU organizational database. My selection of documents began with EU *Cybersecurity* and *Global Strategies* and proceeded in line with the interpretivist criterion of 'research relevance', of which was established through the preliminary reading of primary source documents and secondary literature. The process of generating data and analyses was iterative; a preliminary reading of such documents yielded references to other important concepts, organizations, and policies, and this directed my further research.

To guide my discourse analysis, I referred to Bacchi and Goodwin's interpretive tool, 'What is the Problem Represented to Be?' (WPR), which elicits a sequence of questions for 'opening up policies' for interpretive interrogation.[73] This analysis was conducted with specific attention to the context of key shifts in the EU's cyber policies, to elucidate how the concepts of geopolitics and sovereignty interplay with the EU's cybersecurity discourse.

WPR Analysis – Guiding Questions. Excerpt from Bacchi and Goodwin's (2016) volume	
1	What's the problem represented to be in a specific policy or policies?
2	What deep-seated presuppositions or assumptions underlie this representation of the 'problem'?
3	What is left unproblematic in this problem representation? Where are the silences? Can the 'problem' be conceptualized differently?
4	How has this representation of the problem come about?
5	What effects (discursive, subjectification, lived) are produced by this representation of the problem?
6	How and where has this representation of the 'problem' been produced, disseminated, and defended? How has it been and/or how can it be disrupted or replaced?

Table 2. WPR Analysis (Bacchi and Goodwin, 2016). [74]

Specifically, documents were analysed for discourses pertaining to the following broad topics relevant to my interpretive analysis: representations of cyber threats or issues; representations of cyberspace as a political/economic/social/geopolitical/security environment; representations of sovereignty, as it relates to the EU, its member states, or other state actors; descriptions of 'solutions' to cyber 'problems'; past, present, and future representations of the EU as a security actor in cyberspace; and EU priorities in cyberspace (including policy goals, ambitions, relations with other actors). In these discursive contexts, I elucidated key ideas and themes (*in Appendix 2.2*) which in turn informed my theory building.

Furthermore, to explore how EU policymakers engaged with the strategy of 'othering' throughout various time periods of the analysis, my analysis was informed by Derrida's method of deconstruction.[75] Given that language can be understood as a 'system of differential signs', an actor's identity is established through creating meaning through a series of juxtapositions,

[73] Carol Lee Bacchi and Susan Goodwin, *Poststructural Policy Analysis: A Guide to Practice* (Palgrave MacMillan, 2016).
[74] Bacchi and Goodwin.
[75] As laid out by Lene Hansen, *Security as Practice: Discourse Analysis and the Bosnian War*.

'where one element is valued over its opposite', or Other (Derrida 1976, 1978).[76] My analysis accordingly traced these two dimensions of identity formation: through the *process of linking* (or positive association) and *the process of differentiation* (constructing the Other).[77]

Interviews

To corroborate and clarify my textual analysis, I conducted seven interviews with EU policy elites situated across several of the EU's cybersecurity policy communities. Participants[78] were recruited from the following policy communities: the EEAS, the EU Commission, consultation groups to the European Council (e.g. COREPER I and the Political and Security Committee), and EU affiliated think tanks, viz. the European Council on Foreign Relations (ECFR) and the European Union Institute for Security Studies (EUISS). Recruitment criteria was on the bases of 'research relevance' and 'snowballing' (whereupon further participants were contacted using participants' recommendations).

Interviews were semi-structured, during which participants were asked questions regarding their role within the EU cybersecurity policy development process, which concepts and ideas are/were 'most important' to EU cyber policy development, and the most influential factors for the EU's cyber strategy development. I also asked more specific questions, tailored to their professional experience and particular response.[79]

Interviewees[80] were affiliated with national, intergovernmental, and supranational bodies involved in EU cybersecurity policy development (Figure 3.6) and consisted of national

[76] Hansen.
[77] Hansen.
[78] All interviewees opted to be anonymously quoted, and in accordance with their consent, I cannot disclose their specific positions.
[79] Given my positionality as a graduate research student and in line with research ethics requirements, there were no discussions about national security or politically sensitive topics during the interviews. However, this did not disadvantage my study. For one, the analytical focus is on the EU level, which is less concerned with national security issues, and the goal was not to uncover how each interview 'secretly felt' about cybersecurity on a personal level, but rather how the topic was approached from a broader institutional perspective, within their professional community. Particularly, the aim was to identify patterns of association, including chains of connotations and storylines which have been reproduced about the EU's role in cyberspace—or alternatively, key areas of contestation and ideational disruption in policy communities—by policymakers situated across various EU institutions.
[80] They will be referred to as follows: Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; Interviewee E, interview by author, virtual (online video),

civil servants, Member State Representatives, EU diplomats, EU Commissioners, and cyber policy experts. Some interviewees had professional experience in multiple (relevant) institutional bodies; hence, the number of institutional bodies exceeds the number of interviewees.

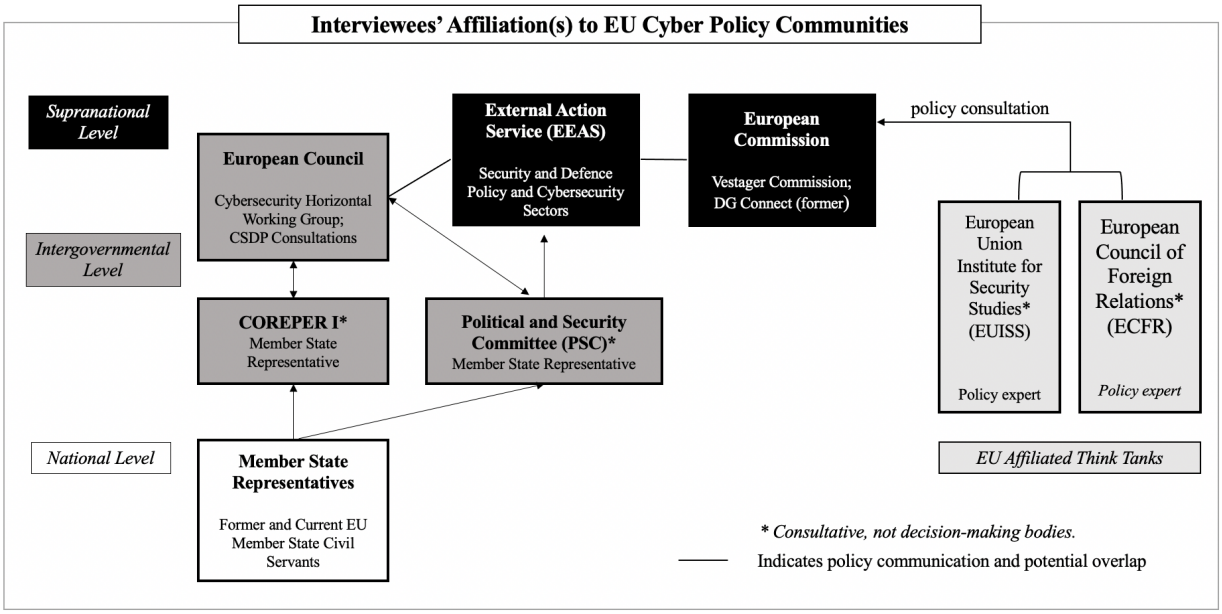


Figure 3. Interviewees' affiliations to EU cyber policy communities.

Responses were analysed for intertextual linkages (such as quoting other texts, reproducing catchphrases or concepts originating in other textual sources), with particular attention to processes of linking and differentiation (to explore their engagement with othering). This process of situating texts within and against other texts, or *intertextuality,* reveals how a particular text, such as a strategy document, is embedded within the broader political and social discourse surrounding the topic.[81]

Given that the findings of this study are predominantly based upon the realm of the EU's *official* discourse, they can only paint a limited picture of the internal dynamics, such as internal discussions or discursive struggles which could have played out 'behind the scenes'.

March 25, 2021; Interviewee F, interview by author, virtual (online video), April 15, 2021; Interviewee G, interview by author, virtual (online video), April 16, 2021.

[81] Hansen, *Security as Practice: Discourse Analysis and the Bosnian War*.

Thus, interviews helped to increase my *exposure* to research sites. By providing an 'inside' perspective on EU cyber policy development from various institutional contexts, interviews were critical for clarifying internal institutional dynamics relevant to the cyber policy formation process, and for identifying areas of discursive struggle within or across policy settings not visible in official EU policy or strategy documents. This exposure enabled me to increase the trustworthiness of my empirical findings through identifying the level of 'explanatory coherence' of the data I generated; that is, 'the consistency of the evidence from different sources.'[82] To this end, interviews helped to explore the possibility of this 'invisible' ideational contestation and overlap, although this was limited to the small number of interviews.

Access to research sites was further curtailed by pandemic circumstances, which added barriers to participant recruitment.[83] Broadening the scope of interviewed policymakers (both current and former) and the exposure to other EU cyber policy settings would benefit this interpretive analysis; for one, it would offer a richer and deeper account of the 2009-2020 timeframe and help to uncover further internal dynamics of EU cybersecurity policy. It would also enable me to gain more exposure to the number of institutions involved in EU cybersecurity development (*as listed in Appendix 2.1*).

In focusing upon EU policy elites, this study undertakes an 'inside-out' approach to exploring EU self-narratives in its cyber policy discourse. A valuable extension to this research would be to examine how 'outsiders' (non-EU actors) have discursively constructed the EU, to explore more thoroughly how social recognition and interaction with the EU's 'constitutive outside' informs its own self-identification and responses to ontological insecurities. Promising empirical cases would include the recipients of the EU's cyber partnership funding (countries in its Southern and Eastern Neighbourhoods), and the US, given its significant security

[82] Schwartz-Shea and Yanow, *Interpretive Design: Concepts and Processes,* 108-109.

[83] Many potential participants were extraordinarily occupied with the COVID-19 pandemic, which has taken place during the two years in which this research was conducted. The pandemic also precluded travel to research sites, thus requiring interviews to be conducted remotely, through online software.

relationship with Europe. I hope to explore the aforementioned suggested extensions and limitations to this study in my future DPhil research project.

Conclusion

In conclusion, I have argued here that a theoretical framework centred upon ontological insecurity makes it possible to explain the prevalence of geopolitical and sovereigntist language in contemporary EU cybersecurity policy. It identified three key loci of ontological insecurities and three strategies which it argues to have implicated the EU's adoption of geopolitical and sovereigntist language. Indeed, as I will empirically demonstrate in the following chapters, how the EU has responded to unfolding dynamics of ontological insecurity in cyberspace has implicated its evolution as a cyber actor and the course of its cybersecurity strategy in distinctive ways.

Chapter IV - Delegitimization

This chapter argues that EU policymakers' responses to insecurities in cyberspace during the 2009-2013 period were broadly self-reflexive and autobiographical, which encouraged EU policymakers to draw upon a particular strategy of temporal othering: the *delegitimization* of geopolitics. Particularly, the securitization of EU cyber policy created internal pressure for the EU to take on a more active role in cyberspace, which in turn introduced existential questions about the EU as a cyber actor. These policy debates, and the ontological insecurities underlying them, shaped the trajectory of the EU's first cybersecurity strategy, leading to the strategy's focus upon inward-looking regulatory and legislative measures, and its passive, vague vision for the EU's role in cyberspace.

The Securitization of Cyberspace

European policymakers' securitization of cyberspace paved the way for the convergence of EU 'cyber policy' with 'security' and thus the formalisation of *cybersecurity* as a distinctive EU policy area. Prior to the mid-2000s, issues in cyberspace were not viewed as key challenges to the EU's security.[1] Instead, the EU's orientation towards 'network and information security' (NIS) in cyberspace was dominated by a regulatory-oriented, economic logic[2] and a focus upon transnational or non-state actors, in which terrorists and organized criminals were constructed as the main perpetrators of threats.[3]

However, this particular discursive construction changed in response to the 2007 cyberattacks targeted at Estonia, which was a triggering event for the securitization of cyberspace in the EU cyber policy context. Subsequently, EU policy discourse shifted in large

[1] Secretary General/High Representative, A *Secure Europe in a Better World: European Security Strategy,* Pub. L. No. PESC 787 (2003), https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf.
[2] Christou, "The Collective Securitisation of Cyberspace in the European Union."
[3] Council of the European Union, *Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems,* Official Journal of the European Union L 69 (2005): 67–71.

part from the notion of *computer-* or *information security* to *cybersecurity*. Whereas the former focused upon *technical* discourses in the context of computer science, the latter marked a turn to incorporating 'cyber' into the 'specialized arena of [trans]national security'.[4]

Through exploring EU policymakers' responses to the Estonia cyberattacks, it becomes clear how the securitization of cyberspace introduced existential questions about the EU's position as an actor in cyberspace and its responsibilities as the provider of economic security for its Internal Market. As well, it reveals the delegitimization of geopolitics at the EU level, whereby overt geopolitical discussions were sequestered to the national level or outside of official EU contexts.

The Estonia Cyberattacks

On 27 April 2007, Estonia was barraged by distributed denial-of-service (DDos) cyberattacks, which took down crucial online services, including banking services and government websites. The cyberattacks were a strategic Russian response to Estonia's decision to relocate and later excavate the Bronze Soldier Memorial, a Soviet-era war statue in Tallinn (NATO Cooperative Cyber Defence Centre of Excellence, 2018).[5]

These attacks were a 'wakeup call' for Estonian government officials, and the event has since spurred the country to become a leader in cybersecurity policy within the EU.[6] More broadly, the attacks underscored to EU policymakers that cyberspace could be exploited by actors to pose significant threats to EU citizens' economic, social, and democratic security.[7] This sentiment was expressed by the EU Information Society and Media Commissioner,

[4] Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53 (2009): 1155–75, https://academic.oup.com/isq/article/53/4/1155/1815351; Helen Nissenbaum, "Where Computer Security Meets National Security ," *Ethics and Information Technology* 7 (2005): 61–73, https://doi.org/10.1007/s10676-005-4582-3.

[5] NATO Cooperative Cyber Defence Centre of Excellence, "2007 Cyber Attacks on Estonia," 2007.

[6] Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021.

[7] European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection,* (Brussels, 2009).

Viviane Reding, who stated that 'We have to wake up our governments […] if people do not understand the urgency now, they never will.'[8]

To a large extent, European policymakers' responses to the Estonia cyberattacks were concentrated within disparate strategic communities at the Member State/national level[9] as opposed to EU-level policy discourse. These discourses demonstrated widespread conceptions—albeit at the national level—that the attacks entailed a geopolitical dimension. For some Member States, the attacks reinforced their concerns about the connection between cyber threats and the broader geopolitical tensions in the EU's neighbourhood.[10] Indeed, the Estonian government stated that these cyberattacks were 'a blatant attack not only on Estonia's sovereignty, but also on the entire European Union.'[11] Reflecting upon the attacks, a French government official remarked, 'It thus appears necessary for states to plant the flag in the spaces they occupy in order to exercise all their sovereign functions, colonize virgin spaces, and be prepared to confront adversaries in this [cyber]space'.[12] The Estonian cyberattacks furthermore encouraged several European Member States to prioritize their development of cyber capabilities, including France and the (former Member State) United Kingdom.[13]

Nevertheless, policymakers' constructions of the attacks through a Westphalian framework (such as the aforementioned French statement) came into tension with what made the attacks so successful: their *evasion* of Westphalian-based international law and security constraints. Whereas one EU official underlined that, 'The Estonians are not alone with this problem. It really is a serious issue for the alliance as a whole,' there was an awareness that NATO 'does not define cyber-attacks as a clear military action' (Estonian defence official,

[8] As quoted in Christou, "The Collective Securitisation of Cyberspace in the European Union," 286.
[9] Interviewee B, interview by author, virtual (online video), March 11, 2021.
[10] Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee F, interview by author, virtual (online video), April 15, 2021.
[11] NATO CCDOE, "2007 Cyber Attacks on Estonia", 56.
[12] Stéphane Dossé, cited in Douzet, "Understanding Cyberspace with Geopolitics."
[13] Douzet.

2007).[14] Thus, NATO's decision to not undertake a military response against Russia was unsettling for European members of the security alliance, stoking the impression that EU Member States could not rely upon the alliance to respond to a 'heavy attack' on a 'sovereign state' in cyberspace (Estonian Prime Minister Ansip, 2007).[15] NATO's response to the attacks thus perpetuated the idea that EU Member States were increasingly vulnerable to Russian geopolitical motives in cyberspace without a firm EU or NATO deterrent.[16]

Nonetheless, official EU-level acknowledgement of the 'geopolitical dimension' to the Estonian cyberattacks did not emerge until years later (after 2013).[17] The event was later recalled by officials, media, and academics as an emblematic example of state geopolitical activities in cyberspace[18]—a sentiment echoed by interviewees, who confirmed that the event marked a clear 'turning point' in EU cybersecurity policy circles.[19] Most recently, the Estonia cyberattacks were referenced by High Representative Josep Borrell at the EU's 2020 Cyber Forum. Asserting that 'cyber issues are geo-political in nature and have a strong security dimension', he recounted that, '[c]yber-attack[s] can leave a country crippled within seconds. Think of […]the attacks that stopped people from accessing their own money in Estonia in 2007.'[20] Therefore, despite the concept's invisibility in official EU discourses during this period, it is clear that the Estonia cyberattacks shaped the EU's understanding of geopolitics in cyberspace. As one EU official noted, geopolitical discussions had been occurring for years, but 'they were not that much exposed' until 2018.[21] Geopolitical ideas were clearly available

[14] As quoted in Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia ," The Guardian, May 17, 2007, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

[15] Andrus Ansip, "Prime Minister Andrus Ansip's Speech in Riigikogu," Estonian Government Website, 2 May 2007, https://www.valitsus. ee/en/news/prime-minister-andrus-ansips-speech-riigikogu.

[16]Finnish cyber expert, Mikko Hyppoenen, as quoted in Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia."

[17]European Parliament, "European Parliament Resolution of 24 May 2007 on Estonia" (2007), https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0215+0+DOC+XML+V0//EN.

[18] Perhaps the closest suggestion of geopolitical intent was the EP's May 2007 *Resolution on Estonia* which acknowledged the political and *historical* geopolitical dimensions of the attack, particularly its relevance to the Soviet Union's illegal incorporation of the Baltic States, including Estonia, into the Soviet Union. Refer to: European Parliament.

[19] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021; Interviewee F, interview by author, virtual (online video), April 15, 2021.

[20] Josep Borrell, "Cyber Diplomacy and Shifting Geopolitical Landscapes," European External Action Service, September 14, 2020, https://eeas.europa.eu/headquarters/headquarters-homepage/85069/cyber-diplomacy-and-shifting.

[21] Interviewee A, interview by author, virtual (online video), March 5, 2021.

to EU policymakers, at least at the national level; however, it appeared that they were not *acceptable* to discuss in an official EU capacity at this point in time.

There are several possible reasons for why the EU itself did not adopt geopolitical language to respond to the Estonian attacks. For one, before to the enactment of the Lisbon Treaty in 2009, the EU had less foreign and security competencies empowering it to act on behalf of its Member States. Lacking an external relations arm until 2010, there was no clear mechanism at the EU level to produce a foreign policy response. As well, attribution was a prickly issue, due to the dearth of concrete evidence implicating Russian state involvement in the cyberattacks and uncertainty about how to apply international law to such an incident.[22] Yet, while the underdeveloped status of EU external relations was an important factor for explaining the EU's lack of response during 2007 and 2008, this cannot sufficiently explain why geopolitical language remained largely absent throughout the 2009-2013 period, *after* the EU acquired significant competences in foreign and security policy and its own external relations arm (in 2010).

Therefore, this chapter explores the significant ontological dimension which contributed to the absence of geopolitical language in EU policy discourses during this period in time. As I demonstrate in the following sections, ensuing policy discussions in Europe from 2009 to 2013 reveal autobiographical insecurities about the EU's capacity to fulfil its established role as an economic security provider in cyberspace and conceptual disagreement about the fundamental features of cyberspace, which encouraged policymakers' engagement with the strategy of temporal othering.

[22] Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia."

Autobiographical Insecurities

Underlying EU policymakers' progressive securitization of cyberspace were pronounced *autobiographical insecurities* about the EU's role (and identity). At both the horizontal and vertical governance levels, the EU's extant identity was destabilized by internal contestation about how to conceptualize cyberspace as an environment and the EU's place within it. In grappling with these existential questions, policymakers approached cyberspace through a predominantly *self-reflexive* orientation, which considered how the EU should position itself relative to its constitutive Member States and its broader existential purpose in the increasingly securitized cyber environment.

In particular, cyber policy discussions about borders reveal the interplay between the EU's autobiographical insecurities on the one hand, and uncertainties about the environmental features of cyberspace on the other. Vertical communication between the Member State and EU levels was rife with varying perspectives about whether a 'European'/regional approach should be taken to cyberspace compared to a national/global approach. In one such debate in 2010, the UK Government's position about whether it was 'sensible to develop European-centric approaches at all,' was the following:

> 'A European-centric approach will by its nature be able to achieve more within Europe, even if it is limited in the issues it can address (some issues—especially around security may be reserved for Member States). An overly prescriptive European approach could also be problematic.' [23]

This vision confines the scope of EU action in cyberspace to internal *European* matters and discourages the EU's involvement (as the embodiment of the European-centric approach) in global cyberspace or matters of security. The UK justified this position on the grounds that 'the Internet operates as a global phenomenon and does not recognise borders,'—therefore,

[23] European Union Committee, *Protecting Europe against Large-Scale Cyber-Attacks*, House of Lords Publications (London, 2010), 5.

cyberspace does not warrant a European-centric focus. [24] According to the UK's position, the lack of borders in cyberspace implies that there is no *internal European (cyber)space*—and therefore no grounds for an EU role in global cyberspace whatsoever.

An EU Commissioner vehemently rebutted this position, arguing that without EU involvement, 'there is no possibility for Europe as a region to cope, to work in the globalised environment of electronic communication networks and services unless there is first a kind of unified way of approaching the problem.'[25] The Commissioner thus re-established the relevance of Europe by engaging in positive form of othering—emphasizing the UK's membership in the European region, and its part in a European, unified whole. Furthermore, the notion of 'coping as a region' is a response to the EU's existential anxiety about its conception as a security provider. It frames the EU's role as a coordinator and rules-setter as not only valuable, but *necessary* for the ability of all European States to survive in cyberspace. Thus, to justify the EU's continued existence, the Commissioner responded by engaging with *temporal othering*. Warning that a lack of European approach would lead to 'not coping as a region' in cyberspace recalls the paralyzing state of disunity and conflict that defined Europe's *past* and the reason for the EU's formation as an entity in the first place.

Significantly, debates about the EU's role in cyberspace were not only shaped by various internal approaches to European integration (such as the British position above), but also ontological approaches to cyberspace itself. While policy incoherence is a widely known (and studied) problem for the EU, cyberspace is distinctive for the level of *ontological* disagreement it elicits for EU policymakers.[26] A 2009 report published by the EU's General Secretariat noted the lack of shared agreement on what constituted cyberspace—let alone cybersecurity—amongst EU policymakers and reiterated the need to establish a formal definition.[27] In its

[24] European Union Committee, *Protecting Europe against Large-Scale Cyber-Attacks*, House of Lords Publications (London, 2010), 5.
[25] European Union Committee.
[26] By comparison, few EU officials would disagree about the *fundamental* nature of 'sea' or 'air' as strategic domains..
[27] Jean-Pascal Zanders, "Cyber Security: What Role for CFSP?," *European Union Institute for Security Studies* (Brussels, 2009).

efforts to establish the 'scope' of the problem, a 2010 European Organization for Security (EOS) White Paper (rather unhelpfully) pronounced that the 'simplest definition of cyber security is the "security of the cyberspace".'[28] Reflecting scholarship about this topic (as mentioned in Chapter 2), the 'complex' nature of 'the cyberspace' was a consistent consideration for producing solutions to EU policy problems, both in EU think tanks and institutions.

At the horizontal level, the EOS and the Council of the EU advanced two competing conceptual approaches to 'borders' in cyberspace, each of which constructed the EU's role in a particular way. On the one hand, the EOS conceived of 'the cyberspace' as distinct from 'the real world' (2010), thus embedding a sense of unreality to the meaning of cyberspace. Given that geopolitical activities are firmly grounded in the 'real (physical) world', it can be inferred that, for the authors of this document, geopolitical logics did not serve as the prominent conceptual 'coordinates' through which to make sense of cyberspace. This conceptual approach to cyberspace as non-geopolitical is compatible with the EU's historical representation as a post-Westphalian, non-geopolitical actor.

In stark contrast with the EOS, the Council of the EU conceived of cyberspace as *space controllable by states* during this period. Specifically, it asserted that states should 'protect that part of cyberspace for which they are responsible.' [29] In so doing, European states' territorial sovereignty was mapped onto cyberspace as the framework through which cybersecurity should be approached within the EU context. Thus, the Council expected cybersecurity challenges to cross the internal/external dimensions and pillars of the EU due to its cross-border nature.[30] However, it believed that cyberspace did not bring about the dissolution of boundaries on the whole.

[28] European Organization for Security, "Towards a Concerted EU Approach to Cyber Security," 2010, 27.
[29] Zanders, "Cyber Security: What Role for CFSP?", 2.
[30] Zanders.

Comparing these approaches to that of a third policy community—the EU Commission—reveals further ontological dissonance about the spatial character of cyberspace on account of its piecemeal adoption of the previous two views. This is demonstrated within the Commission's 2010 *Digital Agenda for Europe*, which voices a conception of cyberspace more closely aligned with the EOS' perspective, yet one that draws upon ideas held by the Council. Like the EOS, it describes cyberspace as a 'borderless' domain, making the argument that online barriers to *markets* should accordingly be struck down. However, it also recognized the strategic importance of the internet and the necessity for including an *external dimension* to cybersecurity in order to preserve a European 'digital way of life.' This secondary provision reproduces the Council's notion that European should protect the part of cyberspace for which it is responsible.

This discursive dissensus yields several important insights. First, there are evidently multiple 'alternative representations' of cyberspace and the EU's role as a cyber actor within EU policy communities[31] (three of which were outlined above). Second, this lack of a stable intersubjective meaning of 'cyberspace' has precluded the formation of concrete, unequivocal strategies about cyberspace as a political/strategic domain. Third, these alternative conceptions of cyberspace and the EU's role within it constitute fissures in the EU's construction of its collective Self, and have contributed to its autobiographical insecurity in cyberspace. Fourth, the discursive contestation between various EU policy communities about the EU's position within cyberspace was predominantly *self-reflexive*, and as I demonstrate below, it took place in the context of internal pressure for the EU to take on a more active security role in cyberspace.[32]

[31] European Organization for Security, "Towards a Concerted EU Approach to Cyber Security"; Zanders, "Cyber Security: What Role for CFSP?"

[32] This was reinforced by 2011 Eurobarometer results on *Internal Security,* which revealed that the most respondents (36%) believed that cybersecurity was the policy area in which the EU should become more active, out of all security challenges listed. European Commission, "Eurobarometer Survey on Internal Security : The Economic Crisis and Terrorism Top the Agenda," *Memo*, no. November (2011).

During this period, there were two identifiable 'issues' which elicited autobiographical insecurities for the EU: first, decreasing public trust in using cyberspace for commercial or recreational purposes; and second, the possibility that the Internal Market could become dependent upon other entities for cybersecurity technology.

First, the fact that EU citizens were growing increasingly distrustful of the internet was a significant concern for officials. The Autumn 2010 Eurobarometer Survey found that a *relative majority* of European respondents 'tend to not trust the internet' compared to other sources of information (with only 37% tending to trust the internet, compared to 41% tending to not trust it), with trust levels *declining* since the previous autumn (2009) by 2 percentage points.[33] Furthermore, Eurobarometer data from 2011 and 2013 polls found that a majority of EU respondents believed they had been exposed to cybercrime, with a greater majority holding this belief in the 2013 study.[34]

Both economic and ontological insecurities shaped this concern. Given that critical European economic services (including banking transactions, communications and technologies) were increasingly taking place in the cyber domain, policymakers realized that the EU's Digital Single Market would suffer severe losses if EU citizens avoided conducting business on the internet, with the damage increasing exponentially.[35] This would precipitate the EU's failure to provide security in cyberspace *and* adequate economic security for its Internal Market. As a predominantly 'economic superpower', the EU's ability to provide economic prosperity to its citizens was linked to the EU's legitimacy as a security provider and as a distinctive supranational political entity.[36] Thus, at stake for EU policymakers was not

[33] Standard Eurobarometer, "European Commission EUROBAROMETER 74 AUTUMN 2010 INFORMATION ON EUROPEAN POLITICAL MATTERS REPORT," 2010, http://ec.europa.eu/public_opinion/index_en.htm.

[34] European Commission, "Eurobarometer Survey on Internal Security : The Economic Crisis and Terrorism Top the Agenda"; Special Eurobarometer, "Special Eurobarometer 404 Cyber Security," 2013, http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf.

[35] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2013, https://doi.org/10.4271/2010-01-1021.

[36] Philipp Lutz and Felix Karstens, "External Borders and Internal Freedoms: How the Refugee Crisis Shaped the Bordering Preferences of European Citizens," *Journal of European Public Policy*, February 11, 2021, 1–19, https://doi.org/10.1080/13501763.2021.1882541.

only the EU's material security, but its *ontological security*; if the EU would become incapable of securing its own Internal Market, the EU's basic existence as a credible security provider cyber actor would be called under question. Accordingly, developing further cyber competencies, including the capability to regulate its internal market and protect fundamental rights in cyberspace, was crucial for the EU's credibility in the eyes of European publics.[37] Therefore, the public pressure driving EU policymakers to formulate an EU-level cyber strategy had coalesced around its responsibilities to sustain the Digital Single Market, and thus the imperative for the EU to *continue fulfilling* its historic economic role in cyberspace.

This ontological insecurity was exacerbated by a second pressure—a confluence of 'dependency' anxieties—which were conceived to dispossess the EU of its capacity to ensure its digital economic prosperity (and therefore its *ontological security*) in cyberspace. During the 2009-2013 period, the problem of 'dependency' acquired three distinctive meanings in EU policy discourse: dependency on foreign technologies; dependency on networked information services for essential services within the EU, and the *inter*dependency of critical information infrastructures between Member States. While this discourse contains relational and spatial aspects, the particular *problem* of dependency targeted the EU's 'Self'; its ability to ensure the EU's internal security, independence, and sustain its distinctive European approach to security 'solutions'.

The EOS 2010 *White Paper* highlighted the first form of insecurity, noting that 'the current usage of essentially non-European technologies for cyber security implementations create a dependency of Europe that could be critical.'[38] However, this anxiety is largely directed towards the EU's internal deficiencies: that it was 'falling behind' comparative to its traditional position as a technological leader and problem-solver, as opposed to levelling its attention or

[37] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[38] European Organization for Security, "Towards a Concerted EU Approach to Cyber Security," 14.

threat representation to *relational others*.[39] The second form of dependency anxiety was concentrated upon the vulnerabilities of networked systems of the EU's critical service providers, which 'play an essential role in providing key support services for our economy and society' as 'the security of their systems is of particular importance to the functioning of the Internal Market'.[40] Such anxiety was aggravated by the awareness of *interdependency* between EU Members of the Internal Market—the 'third' dependency anxiety—which 'creates a significant vulnerability to cascaded failure.'[41] This was laid bare in the UK's (2010) *European Union Commission* report:

> '[The] relatively recent shift towards greater *dependency* and reliance on internet based systems and networks across Europe means a change in the approach to critical infrastructure protection that recognises that cyber related risks and attacks could now impact and affect more than just one nation.'[42]

This *interdependency* anxiety therefore warranted a broad 'change in approach', wherein security solutions had to be coordinated beyond the level of the state.

Overall, these 'dependency anxieties' were primarily focused upon the EU's Self. As opposed to constructing external others as threats, EU policymakers worried that the EU would be unable to guarantee economic security in its newfound circumstances of interdependency and networked security. While this was partly attributed to the cyber environment, the policy 'solution' was centred upon buttressing the EU's own capabilities (and those of its Member States) as opposed to external spaces or other actors.[43] This discursive and ideational context influenced the development of the EU's debut Cybersecurity Strategy of the European Union: *An Open, Safe, and Secure Cyberspace* in 2013 (hereafter EUCSS).

---

[39] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*.

[40] Council of the European Union, *Proposal for a Directive 2013/27(COD) Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union*. Brussels, 2013, 4, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.

[41] European Union Committee, *Protecting Europe against Large-Scale Cyber-Attacks*.

[42] European Union Committee, 50, emphasis added.

[43] For this reason, the EU's ontological insecurity response was not relational or spatial othering.

Cybersecurity in the Union: A Humble Beginning

As the first dedicated EU document about cybersecurity, the EUCSS laid out the foundations for cybersecurity as a distinct EU policy domain. While the strategy was a combined effort from then-Home Commissioner Cecilia Malmström, High-Representative Catherine Ashton, and DG Connect Commissioner Neelie Kroes (therefore incorporating both the external and internal aspects of the EU's competence in cybersecurity), the focus of the policy was largely inward-looking.

The inward-looking orientation of the EUCSS can be understood as a response to EU policymakers' concerns about how to ensure the security and prosperity of the EU's Internal Market in the digital and cyber contexts—and therefore, the EU's credibility and ontological security as an actor. As the strategy emphasized, 'Information and communications technology has become the backbone of our economic growth, and is a critical resource which all economic sectors rely on.'[44] Accordingly, the EUCSS prioritized the protection of critical infrastructure within the internal market and the network and information security of European essential services.[45] This orientation served the purpose of reaffirming the EU's *historically established* role as an economic security provider for EU citizens (and Member States), which had become vulnerable to destabilization due to European citizens' growing distrust in the internet and their reluctance to engage with the Digital Single Market.

However, the *specificities* of the EU's role vis-à-vis cyberspace were left equivocal in the EUCSS, due to competing visions about the EU's role as an actor beyond reinforcing its existing prerogatives (and competences) towards the Internal Market. While the strategy envisaged the EU as having a secondary role to Member States in matters of cybersecurity, this positioning was vague and somewhat contradictory. The document emphasized that, due to the

[44] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 2.
[45] European Commission and High Representative of the Union for Foreign Affairs and Security Policy.

leading role of the private sector and the 'diverse range of actors involved, centralised, European supervision is not the answer.'[46] Nevertheless, while recognizing that Member States governments had significant roles to play, it stated that 'an effective national response would often require EU-level involvement.' [47] Altogether, the document belied the lack of 'collective vision' about cybersecurity at the EU level during this period.[48]

Furthermore, ontological dissensus regarding the *nature* of cyberspace as an environment implicated the EUCSS' representations of threats and insecurities in cyberspace, which were described in such an all-encompassing manner that they were nearly meaningless. In broad overtones, the EUCSS noted that, 'Threats can have different origins — including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.' [49] The EUCCS' lack of conceptual clarity was worsened by its omission of a formal definition of 'cybersecurity.' Overall, the EUCSS reflected enduring ontological dissensus surrounding the global nature of the EU's role in cyberspace and its involvement in issues traditionally associated with national security (including geopolitical issues), prescribing a relatively vague and reactive role for the EU in cyberspace. Moreover, it was emblematic of how geopolitical concepts remained delegitimized in official EU discourse: despite advancing an overly inclusive conceptualization of the origins of security threats in cyberspace, geopolitical motives or tactics were notably absent from this list.

The Delegitimization of Geopolitics

The EU's omission of geopolitical concepts in cyberspace during this period demonstrates that geopolitical ideas were *delegitimized* in EU policy discourses: that is, they were available,

[46] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 17.
[47] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 17.
[48] Carrapico and Barrinha, "The EU as a Coherent (Cyber)Security Actor?"; Sliwinski, "Moving beyond the European Union's Weakness as a Cyber-Security Agent."
[49] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 3.

but not acceptable in official contexts. Compared to the issues of cyberattacks and cybercrime, geopolitical issues were scarcely discussed in EU-level diplomatic settings during the 2009-2013 period.[50] Moreover, when such issues were discussed within the Commission and the EEAS, there was no clear agreement as to how the cyber environment could be geopolitical.[51] Subtle references to geopolitical concepts in official documents—if at all present—were vague and contradictory. For example, the Commission's *Digital Agenda for Europe* (2010) affirmed that 'the digital age is neither "big brother" nor "cyber wild west".[52] Yet, a Commission Communication on *Critical Information Infrastructure Protection* (2011) published shortly thereafter noted that the:

> 'global geo-political dimension [of new technological threats] is becoming progressively clearer. We are witnessing a trend towards using ICT [information and communications technology] for political, economic and military predominance, including through offensive capabilities.'[53]

These constructions elicit a contradictory image of cyberspace: whereas the first description offered a comparatively more reassuring, non-conflictual conception of security in a digitalized world (through its assurance that cyberspace was *not* a cyber wild west), the second text stressed the increased geopolitical dimension to 'new technological threats', invoking a framing of the cyber environment often articulated by 'Digital/Cyber Wild West' discourses elsewhere.[54] As a result, apart from vague and contradictory characterizations of the cyber environment, official engagement with geopolitical concepts was implicit or notably absent from EU cybersecurity documents during this period. This reflects one EU policy

[50] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021.

[51] Interviewee A, interview by author, virtual (online video), March 5, 2021.

[52] European Commission, *A Digital Agenda for Europe Communication 5 No. 245 final/2,* Brussels 2010, 16, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

[53] European Commisssion, C*OMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection 'Achievements and next Steps: Towards Global Cyber-Sec*, Brussels, 2011, 3, http://publications.lib.chalmers.se/records/fulltext/245180/245180.pdf%0Ahttps://hdl.handle.net/20.500.12380/245180%0Ahttp://dx.doi.org/10.1016/j.jsames.2011.03.003%0Ahttps://doi.org/10.1016/j.gr.2017.08.001%0Ahttp://dx.doi.org/10.1016/j.precamres.2014.12.

[54] As a competitive, power-politics 'free for all'—in Rovner and Moore, "Does the Internet Need a Hegemon?"; Chris Demchak and Peter Dombrowski, "Cyber Westphalia : Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs*, 2013, 29–38.

expert's belief that, prior to 2014, the EU had never really considered its actions in geopolitical terms.[55]

The delegitimization of geopolitics was also demonstrated by the fact that, despite the flurry of national-level discussions post-Estonia cyberattacks, there was no mention of geopolitical issues in the EUCSS. Indeed, as European discourses about the Estonia cyberattacks reveal, cyber-geopolitics was perceived largely through the prism of the national level and on the basis of Westphalian notions of state sovereignty during this period of time. Reproducing the UK's position on cybersecurity to a notable extent, this Westphalian orientation encompassed the belief that geopolitical threats (and security issues in cyberspace more generally) should foremost be addressed in a national security context.

Conclusion

This chapter argued that the EU's experience with autobiographical ontological insecurities facilitated the continued *delegitimization* of geopolitics in EU official discourse. It traced two dynamics occurring during the 2009-2013 period: the securitization of cyberspace, and the emergence of primarily *autobiographical* insecurities about the EU's role in cyberspace. These dynamics provided the impetus for further policy discussions about the EU's role in cyberspace and paved the way for the EU's development of its first dedicated cybersecurity strategy. During this period, the discursive contestation amongst policymakers was primarily self-reflexive and brought about a largely inward-looking cybersecurity strategy for the EU, responding to autobiographical insecurities about its capacity to ensure the security of its Internal Market and EU citizens. Moreover, these dynamics contributed to the lack of visibility—*but not complete absence*—of geopolitical ideas and concepts in EU official cyber policy. By the end of this period, the EU was perceived as a 'passive actor' in the field of

[55] Interviewee C, interview by author, virtual (online video), March 12, 2021.

cybersecurity.[56] As I reveal in the next chapter, EU policymakers' growing conviction that the EU—and Brussels—had to take on a more assertive role in cyberspace as a *security provider* was shaped by transformative events in the EU's wider security environment during the 2014-2017 period.

[56] Interviewee A, interview by author, virtual (online video), March 5, 2021.

Chapter V – Rupture and Reconceptualization

This chapter traces developments from the year 2014 up until the release of the EU's updated cybersecurity strategy in September 2017. It sheds light on a broader trend which unfolded during this time period: the *rupture* of the EU's ontological understanding of the global security environment, and the subsequent *reconceptualization* of the EU's role as a global actor.

This chapter begins by documenting how the EU's experiences with several significant crises in its Neighbourhood, especially the Ukraine crisis, influenced the EU's cybersecurity policy development during this period. Not only did the Ukraine crisis urge EU policymakers to rethink their approach to security, but the conflict had direct links to cyberspace, arousing particular *environmental* and *relational insecurities* about the EU's approach to cybersecurity. To reveal how these insecurities shaped cyber policy development, I focus upon cyber capacity building (CCB) as an illustrative example and trace how policymakers' *spatial* and *relational othering* strategies deployed in the Ukraine crisis were reproduced in the design and delivery of CCB programmes. Subsequently, I demonstrate how multiple crises which occurred during the 2014-2017 created a significant *rupture* to the EU's ontological understanding of its Self, its peers, and its conception of its environment, thrusting the EU into an existential crisis. In response, policymakers *reconceptualized* the EU's identity as a global actor (including in cyberspace). This reconceptualized approach was formalised with the release of a new *Global Strategy for the European Union* (EUGS) in 2016. Consequently, EU cybersecurity policy was reconfigured to become compatible with the EUGS' 'joined-up' strategy, which brought about the further integration of EU cybersecurity policy with the EU's global approach. This ideational context was critical for enabling the later adoption of sovereignty discourse and geopolitical language in the next period.

Erupting Insecurities: The Ukraine Crisis

Until the outbreak of the Ukraine crisis, EU policymakers had hoped that the world would remain peaceful,[1] yet, by 2014, the EU's security environment had changed 'dramatically.'[2] The 2014 Ukraine crisis instigated acute ontological insecurities for EU policymakers, and this experience was critical for triggering a period of ontological rupture for the EU. It was also highly influential to the development of EU cybersecurity policy, due to its direct link with cyberspace as a key site wherein the conflict took place. This is corroborated by interviewed EU officials, who highlighted that Ukraine was a 'turning point' for EU cybersecurity policy (as opposed to other developments during this period).[3] As I will demonstrate below, the crisis elicited strong *environmental* and *relational* insecurities that were connected to cyberspace and the domain of cybersecurity.

The crisis erupted in February 2014, following the decision of the Yanukovych-led Ukrainian government to withdraw from a long-awaited Association Agreement (AA) with the EU—the most extensive stage of economic integration that non-candidate states can reach with the Union.[4] The signing of the AA was perceived as a threat by Russia into its traditional sphere of influence, or 'Near Abroad', and it had placed significant pressure on Ukraine to withdraw.[5] Public protests erupted in Ukraine's Euromaidan square to contest Ukraine's withdrawal from the AA, which in turn precipitated the instalment of a new, pro-EU Ukrainian

[1] Interviewee D, interview by author, virtual (online video), March 18, 2021.

[2] EEAS, "Food-for-Thought Paper 'Countering Hybrid Threats'" 2015, no. May (2015): 8, http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15. pdf.

[3] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021

[4] For a full timeline of these attacks and the crisis, refer to Marie Baezner, "Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict" (Zurich, 2018), www.css.ethz.ch., pages 9-11.

[5] Carmen A. Gayoso, "Russian hegemonies: historical snapshots, regional security and changing forms of Russia's role in the post-Soviet region," *Communist and Post-Communist Studies* 42 no. 2 (2009): 249, https://ac.els-cdn.com/S0967067X09000208/1-s2.0-S0967067X09000208-main.pdf?_tid=c8149fe5-c305-4735-bf8a-7dfd969db0e9&acdnat=1521211728_8d346f03b0d1b69ae6fe5e62df98c8cc.

government.[6] In response, Russia annexed Crimea, claiming that it was for the protection of Russian-speaking populations.[7]

However, months before Ukraine withdrew from the AA and the Yanukovych government fled to Russia, Russian hacker groups had been bombarding Ukraine websites with DDoS attacks, targeting sites 'critical' to Ukraine's relationship with Russia as an attempt to discourage the signing.[8] Later, on 2 March, 2014 (three days after the invasion of Crimea), Russian hackers shut down the website of the Ukrainian government and subsequently inserted malware into the electronic systems of Ukraine's Central Election Commission. These activities sabotaged the Crimean election results to support Russia's claim that most Crimeans had voted in support of 'rejoining Russia'.[9] Meanwhile, Moscow had been collecting intelligence through exploiting Ukraine's dependence upon Russian email service providers.[10] As the conflict continued into 2015 and 2015, Russia continued to levy cyberattacks on Ukrainian critical infrastructures; for instance, disabling a Kiev power grid in December 2016.[11] Overall, the crisis was a 'wakeup call' for EU policymakers, who realized that the EU needed to 'step up' its role as a global security actor.[12]

Environmental Insecurities

By demonstrating how cyberspace could serve as a site for geopolitically motivated, hybrid warfare, the Ukraine crisis aroused serious *environmental insecurities* for EU policymakers.[13] It became clear that cyberspace could be used to threaten the EU's

[6] David Cadier, "The Geopolitics of Eurasian Economic Integration," *LSE Ideas*, no. June (2014), http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Geopolitics-of-Eurasian-Economic-Intergration.pdf.

[7] Adrian Pop, "From Cooperation to Confrontation: The Impact of Bilateral Perceptions and Interactions on the EU-Russia Relations in the Context of Shared Neighbourhood," *Eastern Journal of European Studies* 7, no. 2 (2016): 47–70.

[8] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (NATO CCD COE Publications, 2015), http://www.kyivpost.com/content/kyiv-.

[9] Maurer.

[10] Baezner, "Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict."

[11] Baezner.

[12] Interviewee D, interview by author, virtual (online video), March 18, 2021.

[13] Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021.

geographical environment; the EEAS concluded that Russian hybrid warfare had 'compromised Ukraine's territorial integrity and […] strived to destabilise the larger neighbourhood'.[14] This was echoed later that year, when a European Parliament paper attributed the emergence of hybrid cyber operations to the 'changing global environment', citing Russian and Chinese state-backed hacking as prime examples.[15] Furthermore, policymakers realized that cyberspace could be used to exploit actors' dependence on foreign technologies for their own geopolitical aims.[16]

Altogether, the emergence of hybrid warfare tactics in cyberspace during the Ukraine crisis brought about the ontological realization that the dimensions between different *policy domains*—such as civil and military, or cyberspace and physical space—were becoming increasingly intertwined. Additionally, the capacity for hackers to penetrate into civilian systems, particularly critical infrastructures such as the Ukrainian power grid, made it abundantly clear that the dimensions between *internal* (domestic) and *external* security were becoming increasingly blurred. As stated by the EEAS in 2015, 'Hybrid threats also demand a fundamentally different mind-set where traditional separation lines between internal and external, defence and homeland security, civil and military affairs are no longer easily applied.'[17] With these revelations, EU policymakers believed that cyberspace as a strategic and security domain had become increasingly unstable and unpredictable.[18]

Taking this into account, EU policymakers reoriented the focus of cybersecurity policy to become more external-facing and cross-dimensional. In 2014, the EU Council designed the Cyber Defence Policy Framework to contend with the growing 'cyber dimension' in many hybrid threats and campaigns.[19] The 2014 framework foreshadowed the EU's subsequent

[14] European External Action Service, *Food-for-Thought Paper: 'Countering Hybrid Threats.'*
[15] Patryk Pawlak, "Understanding Hybrid Threats," 2015, https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.
[16] Baezner, "Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict."
[17] European External Action Service, *Food-for-Thought Paper: 'Countering Hybrid Threats,'*16.
[18] Interviewee D, interview by author, virtual (online video), March 18, 2021.
[19] Politico-Military Group, *Six Monthly Report on the Implementation of the Cyber Defence Policy Framework,* vol. 2016, 2016.

release of the 2016 *Joint Framework on Countering Hybrid Threats,* which outlined the 'cyber' aspect to hybrid conflicts.[20] More broadly, the EU's security and defence agenda was reformed to reflect an ontological understanding of security threats as cross-dimensional, rapidly evolving, and less predictable. The *European Agenda for Security* (2015), expressed, for instance, that 'EU internal security and global security are mutually dependent and interlinked.'[21] Subsequently, the EU's 2016 *Joint Framework on Countering Hybrid Threats* recognized the potential for cyberspace to be leveraged by 'perpetrators of hybrid threats'—including state actors.[22]

What therefore emerged in EU policy discourses following this event was an enthusiastic turn towards the external, relational, and spatial dimensions of cybersecurity. An interviewed EEAS official described this development as unfolding over a three-year time span, whereupon discussions about the external dimension in 2014 evolved into intensified, concrete actions by 2017.[23] This can be partly explained by the fact that, at the time of the crisis, the EU's first cybersecurity strategy (EUCSS) was only a few months old, and it placed a strong focus upon the EU's internal environment, especially its internal market (albeit with some inclusion of 'external elements'). Thus, to achieve a cross-dimensional approach, the external dimension to cybersecurity policy had to be amplified. At the same time, however, this decision reflected then-EU Commissioner José Barroso's belief that, 'we [Europe] cannot retreat from the world. The world needs an open Europe and Europe needs to embed itself in the rest of the world'—an imperative that warranted further EU investment in external relations.[24] Thus, the EU's later release of the *Network and Information Security Directive* in 2016 exemplified this sensitivity

[20] European Commission and HRVP, *Joint Framework on Countering Hybrid Threats: A European Union Response*, Brussels, 2016.
[21] European Commisssion, *The European Agenda on Security*, Brussels, 2015, 4, https://doi.org/10.4324/9780429465918-2.
[22] European Commission and HRVP, *Joint Framework on Countering Hybrid Threats: A European Union Response*, 10.
[23] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[24] Jose Manuel Durao Barroso, *European Commission 2004 – 2014: A Testimony by the President with Selected Documents*, 22, 2014.

to the 'external', despite being intended (in terms of implementation) for internal EU/Member State audiences.[25]

Relational Insecurities

The Ukraine crisis also introduced new *relational* ontological insecurities for EU policymakers. The crisis revealed that Russia was increasingly following its *own* rules in Europe, as opposed to the jointly agreed-upon rules outlined in the 1975 Helsinki Final Act.[26] Indeed, Laine argued that the crisis 'reversed earlier expectations that Russia would be a willing partner in a joint and cooperative security system.'[27] As stated by then-Commission President Barroso, Russia's invasion of Crimea and its actions in the EU's Eastern Neighbourhood was viewed as a form of ideological 'retrenchment' and a 'threat to […] European interests and values.'[28] The EEAS later decried Russian intervention in Ukraine as 'challeng[ing] the core principles of international law.'[29] At the same time, the fact that Ukraine had crumbled under Russian pressure left the impression that there were enduring insecurities in the region, which threatened to destabilize the EU's reputation more broadly. The EEAS noted that Ukraine's withdrawal from the AA enabled Russia to paint the EU as 'not merely as a biased party but also as the instigator of the conflict.'[30]

A prominent response to these insecurities was to engage in *externalisation* of threats as a form of relational othering. Then-Commission President Barroso asserted that, '…[without] EU membership, Bulgaria and the Baltic states would have suffered the same fate at the hands of Russia as Ukraine did in 2014.'[31] His statement reproduced the EU's 'long

[25] European Parliament, *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union,* Pub. L. No. L 194/1, Official Journal of the European Union, Brussels, 2016, https://doi.org/10.2307/j.ctt1xhr7hq.20.

[26] Jussi Laine, "The Ukraine Crisis and Ontological (In)Security: Implications from a Finnish Perspective," in *Ukraine after Maidan - Revisiting Domestic and Regional Security - Soviet and Post-Soviet Politics and Society*, ed. Tomasz Stępniewski and George Soroka (Stuttgart: Ibidem-Verlag, 2018), 65.

[27] Laine.

[28] Barroso, *European Commission 2004 – 2014: A Testimony by the President with Selected Documents,* 276.

[29] EEAS, *Food-for-Thought Paper 'Countering Hybrid Threats*', Brussels, 2015, 2.

[30] EEAS.

[31] As quoted in Viktoria Akchurina and Vincent Della Sala, "Europe and the Ontological Security Dilemma: Narrating the Emerging Eurasian Space," *Europe-Asia Studies* 70, no. 10 (2018): 1638–55, https://doi.org/10.1080/09668136.2018.1546829.

peace' narrative; yet, as opposed to referencing Europe's geopolitical past (as a *temporal* other), he differentiated the EU model to a *relational* other: Russia. It was also spatial, insofar as it established a clear geographical boundary between Russia and the EU's eastern Member States. Framing EU membership as a bulwark against Russian expansionary efforts constructed the EU's internal environment (thus its Self) as secure and *externalised* the threat to the insecure other (Russia). Simultaneously, this narrative constructed Ukraine as *other* than an EU Member, thus dissociating the EU's Self from insecurities in its Neighbourhood. First, by lumping Ukraine in with all the 'others', this strategy ignored the fact that Ukraine had been poised to become an Eastern *partner* to the EU through an *Association* Agreement. Second, by framing Ukraine's lack of EU Membership as the reason for its vulnerability to Russian attack, the EU deflected criticisms about its failure to foresee the conflict or protect Ukraine. That is to say, Ukraine's 'otherness' from EU Member States made it vulnerable to invasion, *not* its attempt to become more closely associated with the EU. Thus, this discursive response also demonstrated how environmental and relational insecurities can become entangled with each other, as anxieties about Russia as an unpredictable actor led to the EU's adoption of a particular spatialized rationale, wherein EU Members were seen as *safer and more secure* than non-Member States caught between Russia and EU borders.

Overall, the crisis made it clear to EU policymakers that Russia's maverick behaviour had become the norm as opposed to the exception. Since 2011, Russia had been advocating for its particular version of 'internet sovereignty' on the global stage [32], which was at odds with the EU's preferred approach of adhering to existing international law.[33] The crisis thus cemented the EU's distrust of Russian efforts to establish 'new rules' in cyberspace, and encouraged EU policymakers to incorporate a cyber component to EU diplomatic efforts.

[32] Sally Adee, "The Global Internet Is Disintegrating. What Happens Next?," BBC, May 15, 2019, https://doi.org/10.1002/esp.1977.

[33] As laid out in European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*

Indeed, after the crisis, the EU-US Cyber Dialogue was made official in 2014,[34] and 'cyber' was incorporated into EU bilateral relations the following year.[35] Moreover, the newfound awareness about hybrid threats post-Ukraine crisis brought about a deliberate reorientation to the dimensions of security. By 2016, there was a clear sense of 'inescapability' of threats in cyberspace, as an EU Commission diagram indicates below (Figure 5).

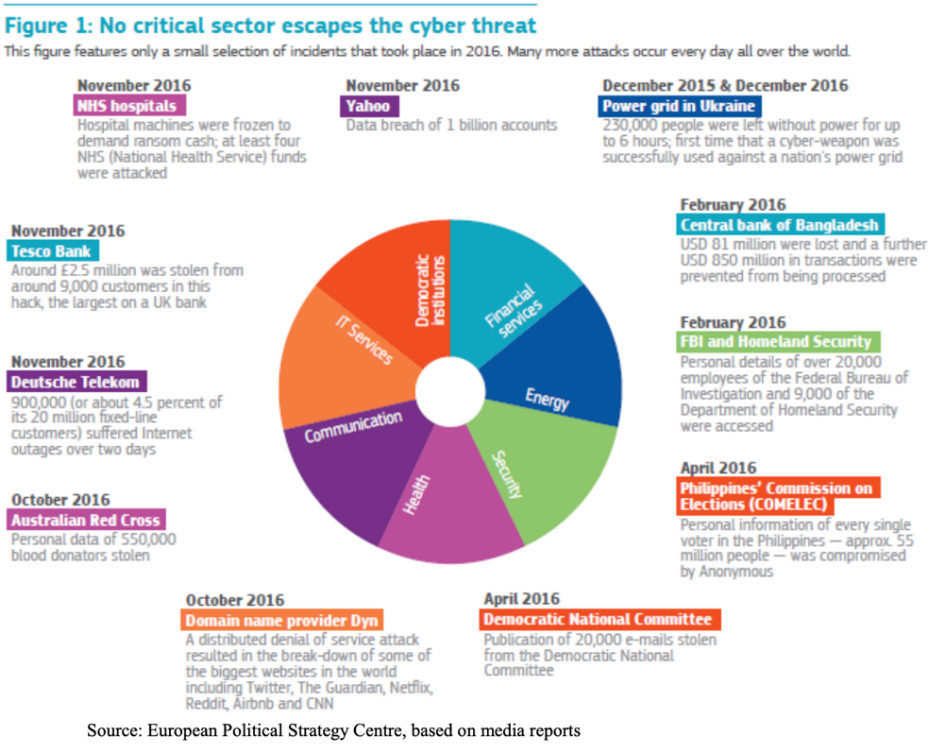


Figure 4. An EU Commission visualization of worldwide cyberattacks in 2016.[36]

Significantly, capacity building emerged as a key policy response to the lessons of the Ukraine crisis. It was considered to be vital for the EU to achieve 'resilience' in its increasingly unstable global environment, which was defined by the EEAS as, 'having the capacity to withstand stress and catastrophe.'[37] In EU cybersecurity policy, resilience had already emerged

[34] André Barrinha, "Virtual Neighbors: Russia and the EU in Cyberspace," *Insight Turkey* 20, no. 3 (2018): 29–41, https://doi.org/10.25253/99.2018203.02.

[35] EU Council, *Council Conclusions on Cyber Diplomacy*, Brussels, 2015, no. February (2015): 1–13, http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

[36] European Commission, "ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries," 5.

[37] EEAS, F*ood-for-Thought Paper: 'Countering Hybrid Threats*", 5. The second prominent response was EU Strategic Communication, which was targeted specifically at fighting 'disinformation in the EU's Neighbourhood'. However, strategic communication was particularly focused upon the Eastern Neighbourhood and Russian propaganda efforts, and it has had a lesser role within the broader context of EU cybersecurity policy. As reported by Interviewee A, interview by author, virtual (online video), March 5, 2021.

as an objective in the 2013 cybersecurity strategy, and the broad goal of 'resilience' has endured over time as a consistent goal in this policy field.[38] However, CCB programmes adopted the discursive strategies of *relational* and *spatial othering* which had emerged in the context of the Ukraine crisis, thus demonstrating the influence of this broader ontological 'rupture' on the trajectory of EU cyber policy.

Spatialization and Externalisation in Cyber Capacity Building

EU CCB programmes reveal how relational and environmental insecurities elicited by the Ukraine crisis influenced the development of cybersecurity policies during this time period. The entanglement of EU policymakers' (relational) insecurities about *neighbours* with (environmental) insecurities about their *neighbourhood*—which had characterized the EU response to the Ukraine crisis—is also revealed in the case of CCB programmes. After the Ukraine crisis, these programmes deployed a combination of spatialization and externalisation in the design and delivery of such projects. Particularly, the relationship between an insecure external environment and unpredictable external others is observable in the EU's focus upon the 'security-development' nexus in CCB programmes. By tracing the catchphrase of 'security-development nexus'—that is, the interplay between the EU's development goals and its security goals—the EU's *spatialized* and *externalised* approach to CCB projects becomes visible. This concept entailed both a spatially targeted approach to development and a significant relational aspect focused upon 'confidence-building' with external neighbours.[39] This approach was justified by a rationale of *externalisation,* which constructed threats as *external* to the EU and largely perpetrated by external actors.

[38] Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*; Christou, "The Collective Securitisation of Cyberspace in the European Union."

[39] Interviewee G, interview by author, virtual (online video), April 16, 2021. See also Renard, "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain."

Only a few months prior to the Ukraine crisis, in November 2013, various EU stakeholders and agencies convened for a CCB conference to establish 'common key concepts' about the programmes.[40] At this point in time, the proposed working definition for CCB was 'support provided to developing nations to increase their access to, and ability to fully benefit from, the internet and other elements of cyberspace.'[41] Consequently, prior to 2014, CCBs were largely oriented around cybercrime and development, and lacked a particular geographical focus beyond targeting third countries.[42] In early 2014, CCBs were considered by EU policymakers as 'not a priority' but they 'should be'.[43] However, this orientation changed following the Ukraine crisis, after which CCB adopted a more *spatialized* approach and it emerged as a key feature in EU cybersecurity policy.

The Ukraine crisis left 'little doubt' for EU policymakers 'about the link between the security of critical infrastructure and human development' in the area of cybersecurity, both in terms of the security of critical services and resilience against cyber threats.[44] Thus, policymakers concluded that a greater focus should be placed upon the nexus between security and development in cyberspace, which called for the prioritization of CCB. Accordingly, since its enhancement under the 2015 European Agenda on Security, *cyber* capacity building has become a key policy in the area of cybersecurity and digital development, and one of strategic importance for the EU's cyber diplomatic efforts.[45] Above other aspects of CCB, development benefits have been emphasized most prominently.[46] For EU practitioners, a key guiding concept for the developmental aspect of CCB is the 'to train principle', which is geared towards

[40] European Institute for Security Studies, "Capacity Building in Cyberspace: Taking Stock (Event Report)" (Brussels, November 19, 2013).

[41] "Capacity Building in Cyberspace: Taking Stock" (Brussels, November 19, 2013), 2.

[42] Countries mentioned in EU CCB reports included: Kenya, Ghana, Pakistan, Nigeria and Sri Lanka; organizations noted included ASEAN, the African Union Commission, and the council of Europe. Patryk Pawlak, "Cyber Capacity Building in Ten Points," March 14, 2014..

[43] Pawlak, 1.

[44] Patryk Pawlak, "Building Capacities for Cyber Defence," *EUISS*, November 2017, 1, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert 26 Cyber development.pdf.

[45] Council of the EU Presidency, *Cyber Capacity Building: Towards a Strategic European Approach*, Brussels, 2016.

[46] Generally, officials have extolled the importance of *developing* cyber capabilities in third countries; CCB's link to fulfilling the 2030 UN Agenda for Sustainable Development; and the EU's established role as a development actor in external relations. As reported by Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

helping partner countries by sharing the lessons the EU has learned in the area of cybersecurity.[47]

Yet, the 'to train principle' in EU CBB projects can also be understood as a form of *spatialization*, in which the EU aims to decrease its environmental insecurities through transforming its external environment to become more compatible with its own, secure model. Echoing Veit Bachmann's observation about EU development initiatives in Africa, the 'to train' principle reproduces the EU's pattern of 'transfer[ing] the modus operandi of the EU's system of political-economic organization to European external relations.'[48] The virtues of exporting European success (albeit under the auspices of universality) are echoed in the Commission's Staff Working Document on *Digital4Development* (2017). This missive details how CCB projects leverage 'Made in Europe' solutions as part of their actions in participating accession and Neighbourhood countries (through the iPROCEEDS, Cyber@EAPII and III projects). This belief mirrors Commission President Barroso's response to the Ukraine crisis in 2014, in which he stressed that 'Europe needs to embed itself in the rest of the world' for its security.[49] To this end, EU officials have regarded Kenya as the model of success for CCB, which recently adopted the EU's 'GDPR-like'[50] data privacy legislation into its national cybersecurity policy framework.[51]

The practice of spatialization in EU CCBs is especially apparent when conditionality is taken into account, which is an *additional* measure to the aforementioned 'to train principle'. Indeed, CCB projects are structured so that EU funding and values are exchanged for partnership with third countries and their *receptivity to the EU's values*, including the EU's normative goal of an open, free, and secure internet. For one, the EU's funding of CCB

[47] Interviewee A, interview by author, virtual (online video), March 5, 2021.

[48] In Luiza Bialasiewicz, *Europe in the World: EU Geopolitics and the Making of European Space* -, ed. Luiza Bialasiewicz (Routledge, 2015), 6.

[49] Jose Manuel Durao Barroso, *European Commission 2004 – 2014: A Testimony by the President with Selected Documents*, 22, 2014.

[50] The GDPR, or the General Data Protection Regulation, is EU legislation passed in 2013 surrounding data privacy and protection.

[51] Interviewee E, interview by author, virtual (online video), March 25, 2021.

programmes for third countries has remained conditional upon their (eventual) signing of the Budapest Convention, which has served as a useful instrument for promoting European cyber norms globally.[52] This conditionality requirement is a well-known policy instrument leveraged by the EU in its Neighbourhood Policy, including within its Association Agreements.[53]

Moreover, spatial othering is laid bare by identifying the *participants* of CCB projects, of which are already subject to the EU's Neighbourhood Policy. As Figure 4 exemplifies, EU-led or funded CCB programmes have been prioritized in the EU's Eastern and Southern Neighbourhoods.[54] These geographically targeted projects include the 'CyberEast' partnerships in Eastern Europe (Figure 4) and the GLACY++ programmes in Africa. To a notable extent, geographical approach of CCB reproduces the EU's logic of 'concentric circles' previously deployed to stabilize its (physical) Neighbourhood, which encompasses the process of transforming the EU's periphery in a concentric fashion through incentivizing proximate countries to uptake EU norms and democratic mechanisms with 'conditionality' instruments.[55] Accordingly, CCB programmes have incorporated a particular *spatial* understanding of the cyber environment in terms of 'European cyberspace' and 'non-European cyberspace.'

[52] Interviewee F, interview by author, virtual (online video), April 15, 2021; see also Renard, "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain."

[53] European Union, *Association Agreement between the European Union and Its Member States, of the One Part, and Ukraine, of the Other Part,* Official Journal of the European Union L–161, no. 2014-02–29, 2014: 1–2137, https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf.

[54] Council of the EU Presidency, *Cyber Capacity Building: Towards a Strategic European Approach*; General Secretariat of the Council, E*U External Cyber Capacity Building Guidelines - Council Conclusions*, Brussels, 2018.

[55]For further reference, see Browning, "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War.'"

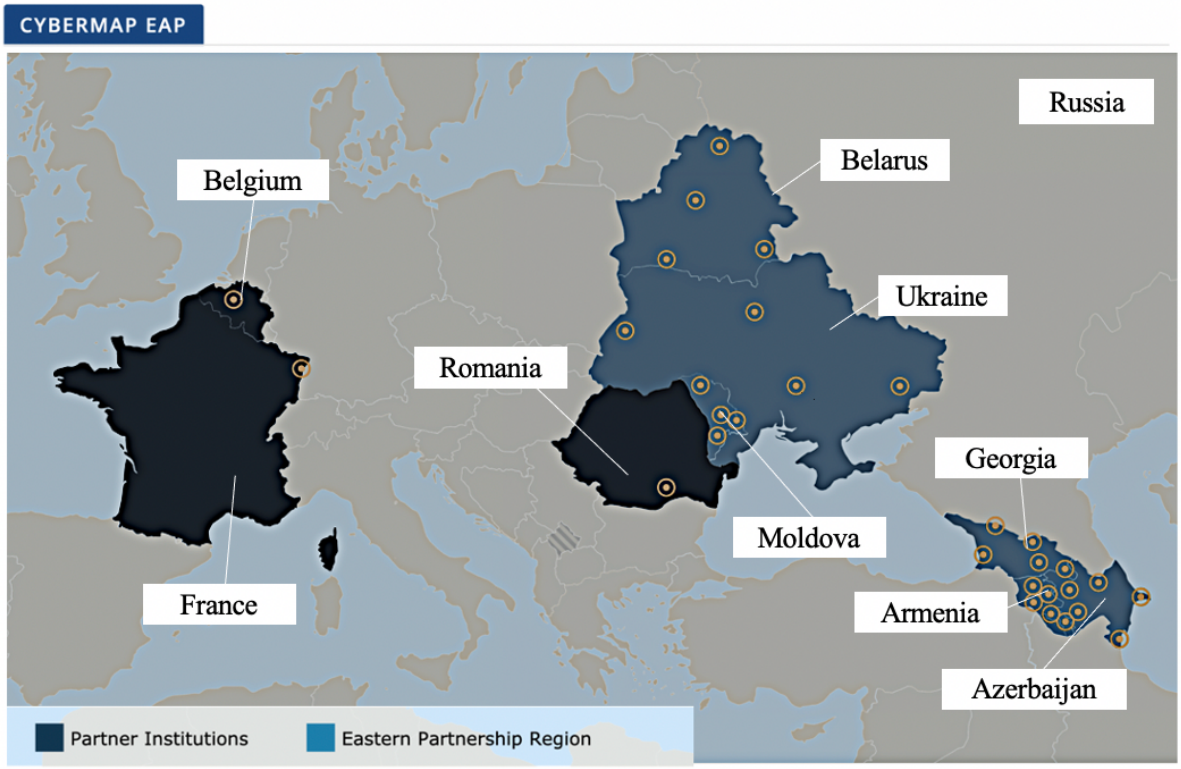


Figure 5. Current map of the CyberEast partnership region. [56]

The logic of *externalisation* has pervaded EU discourses about CCB programmes. EU cybersecurity policies and EU officials have cited the 'borderless' nature of threats or malicious activities in cyberspace as justifying further *external* intervention, particularly, 'enhancing cyber capacity building action under external assistance instruments.'[57] Outside of the EU's conceptual framework of security, this could be seen as peculiar, as if cyber problems are indeed 'borderless', they would not logically merit *external* instruments (which by definition have a bordered aspect), but rather the proportionate use of *all* instruments. However, using 'borderless threats' to justify further external intervention coheres with a key component of the EU's broader security logic, which holds that internal security depends upon external security—or, according to Barroso, as requiring more EU investment into external relations.[58]

[56] European Union Council of Europe, "CyberEast," Council of Europe, 2021, https://www.coe.int/en/web/cybercrime/cybereast. The colour of visual was adjusted by this author for better contrast.

[57] Council of the EU Presidency, *Cyber Capacity Building: Towards a Strategic European Approach*, 3. This rationale was also voiced by the European Commission, *ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries,* Brussels, 2018, 4.

[58] This rationale was voiced by the European Commission, *ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries*, Brussels, 2018, 4.

One interviewee expressed that improving the cyber capabilities of close partners helps the EU from a *geopolitical* perspective, as their vulnerabilities also affect the EU.[59] This echoes the notion of 'my neighbour's and my partner's weaknesses are my own weaknesses', as laid out in the EU's 2016 global strategy.[60] Thus, the borderless nature of cyberspace was cited as a crucial reason for further extending the EU's external assistance to other countries, as it was seen as a way of alleviating its dependency upon others in cyberspace.

At the same time, this approach belies the *relational insecurity* that the origin of the threat predominantly originates from *external* actors that emerged in the context of the Ukraine crisis. In the context of CCB, such insecurities centred around the unpredictability of the EU's neighbours and their (lack of) adherence to established rules of conduct in cyberspace. Interviewed EU officials lamented the lack of clear rules and expectations for safe conduct in cyberspace, which made it difficult to develop a stable understanding of others' behaviour.[61] One policymaker stressed that the EU still needed to understand 'what to expect' from other countries in cyberspace—it had to ask states to 'please present […] how you would interpret different situations [and] how you would apply the international law to particular situations' (Interviewee A, 2021).[62] Another EU official asserted that divergent approaches to what constitutes 'a safe and secure cyberspace' have made it difficult to understand relationship dynamics in the cyber environment.[63] A clear link was drawn to the Ukraine crisis by EU officials' observation that this 'lack of transparency' and unreliable behaviour by other actors has escalated in line with the rapid evolution of hybrid threats in cyberspace.[64]

[59] Interviewee B, interview by author, virtual (online video), March 11, 2021.
[60] European Union, *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy,* European Union, Brussels, 2016.
[61] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021.
[62] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[63] Interviewee D, interview by author, virtual (online video), March 18, 2021.
[64] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021.

By engaging with third countries in order to establish stable expectations about safe conduct in cyberspace, CCB projects have responded to such *relational anxieties*. Indeed, the regional approach to CCB was believed to increase 'confidence building' amongst partner countries and contribute to European regional security, particularly in the Eastern Neighbourhood.[65] Exporting EU values through the 'to train principle'—that is, *externalising* its governance model to third countries—also helps to redress the EU's perceived dependencies upon other actors, an anxiety which had emerged in the earlier phase of policy development (as argued in Chapter IV). Accordingly, the bulk of CCB programmes have focused upon the EU's external environment.[66]

Overall, policymakers' revelations and responses to security threats following the Ukraine crisis influenced how the EU approached cybersecurity policy during this period, as revealed by how CCB took on a distinctly spatialized, externalising form, reproducing and building upon the EU's established spatial approach to its Neighbourhood. For EU policymakers, the utility of this particular approach to cyber policy was reinforced as a result of two other destabilizing developments during this period: the migration crisis, and relations with US President Donald Trump, which exacerbated its extant insecurities. These events, in turn, precipitated ontological rupture for the EU, as it was confronted by an overwhelming cocktail of *autobiographical, relational,* and *environmental* insecurities.

Rupture

As the Ukraine conflict continued to destabilize the EU's Eastern Neighbourhood, the migration crisis in Europe fuelled policymakers' convictions that the dimensions between internal and external security had become increasingly blurred. It reinforced EU policymakers'

[65] This rationale was voiced by the European Commission, *ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries*, Brussels, 2018, 8.

[66] Interviewee F, interview by author, virtual (online video), April 15, 2021.

perceptions of *relational insecurity* and encouraged the logic of externalisation in EU cybersecurity policy.

Beginning in 2015 when a historically unprecedented number of irregular migrants entered the EU, the migration crisis exacerbated an already existing trend of *externalisation,* which centred upon the construction of migrants as grave threats to EU citizens' security.[67] As a consequence of the crisis, several EU Member States suspended the Dublin Regulation, which had legislated the distribution of asylum requests amongst all EU countries, and proceeded to engage in a contentious process of 'internal bordering' along national boundaries. This divisive behaviour sparked intense criticisms that the EU had 'lost control over its borders', which converged with growing public opinion that the EU had insufficient external border controls.[68]

By constructing the EU as unable to control its borders, the crisis called into question a foundational aspect of the EU's capacity as a political actor, and more fundamentally, its *existence,* on two grounds. First, Member States' disagreement about the distribution of asylum claims, including how governments would 'share the burden' of accepting migrants, undermined the EU's self-representation as the global locus of refuge and peace.[69] Second, EU policymakers believed that the EU's incapacity to establish clearly demarcated borders made it vulnerable to instability from the *outside*. This insecurity about its Self was also inherently *environmental*; as the head of the EU-Council during this period, stated, 'a Europe without internal borders can only exist if there are functional external borders'[70]—and the EU had lost control over them. The necessity of 'bordering' the EU relative to outside space is constructed as integral to maintaining freedom of movement—a hallmark of European

[67] However, the securitization of migration has remained a trend since 9/11. In Lena Karamanidou, "The Securitisation of European Migration Policies: Perceptions of Threat and Management of Risk," in *The Securitisation of Migration in the EU* (Palgrave Macmillan UK, 2015), https://doi.org/10.1057/9781137480583.
http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=migr_eipre&lang=en,

[68] Lutz and Karstens, "External Borders and Internal Freedoms: How the Refugee Crisis Shaped the Bordering Preferences of European Citizens."

[69] Akchurina & Sala, 2018). This self-representation was indeed reproduced within several of former Commission President Jean-Claude Juncker's *State of the Union* speeches (2015, 2016, 2017).

[70]Sebastian Kurz, as quoted in Steven Erlanger and Katrin Bennhold, "For Europe, Cutting the Flow of Migrants Challenges Basic Ideals ," The New York Times, July 5, 2018, https://www.nytimes.com/2018/07/05/world/europe/migrants-merkel-kurz-austria.html.)

integration—and thus its political identity. This logic of 'external bordering' therefore underscores the continued importance of a 'constitutive' outside for the EU's internal security. As demonstrated in the previous section on CCB, this externalisation rationale influenced how policymakers approached cyberspace.

Compounding the EU's insecurities during this period was the growing rift in transatlantic relations between Europe and the US, particularly with the 2016 election of President Trump. This deterioration in relations was unsettling for EU policymakers, who relied upon the US to recognize, support—and to an extent, secure—the EU's role in global affairs. It particularly exacerbated the EU's *relational insecurities*; as Commission President Barroso had noted only two years prior that, 'there is no more important partner than the United States [for the EU]'.[71] Trump's approach to transatlantic relations demonstrated to the EU that, on the one hand, 'the continuous presence of the West as the not quite the policeman, but kind of the ordering force in international relations just wasn't secure,' and on the other, that Europe was heavily dependent on the US for security and defence, which was 'a bit of a gamble.'[72] Thus, Washington's aloof relationship with Europe served as an additional push for Member States and officials in Brussels to consider a more active European role in the global security order.[73]

The events explored in this chapter comprised parts of a broader whole of security crises[74] which plagued the EU during this period. Altogether, these events reinforced the impression that the EU was no longer surrounded by a 'ring of friends' but increasingly a 'ring of fire', including within cyberspace—marking a critical period of ontological rupture for the

[71] Barroso, *European Commission 2004 – 2014: A Testimony by the President with Selected Documents,* 23.

[72] Interviewee C, interview by author, virtual (online video), March 12, 2021.

[73] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

[74] Other influential crises include Brexit, instabilities in the EU's Southern Neighbourhood, among others. Tracing these developments, as similarly Malksöo demonstrated in her chronology of EU *security* strategies, 'shows the EU as increasingly anxious to prove its relevance for its own citizens, yet notably less confident about its actual convincingness as an ontological security framework for the EU's constituent members over time.' Maria Mälksoo, "Contemporary Security Policy From the ESS to the EU Global Strategy: External Policy, Internal Purpose," 2016, https://doi.org/10.1080/13523260.2016.1238245.

EU.[75] This insecure political context tipped the balance for EU policymakers, precipitating the *rupturing* of its prior worldview of the external environment as comprising, on the one hand, the US unconditionally supporting European security, and peaceful, rule-abiding international actors on the other. Rather, by 2016, it became abundantly clear that the EU could no longer maintain this 'traditional mind-set' to security, and it was time to reconceptualize the EU's role as a global security actor.

Reconceptualization

Indeed, it was against this political and ideational backdrop—particularly the EU's eroding sense of security in both its internal, bilateral, and international environments—that HR/VP Federica Mogherini (2014-2019) spearheaded the development of the EU's *Global Strategy for the European Union* (EUGS). The ontological imperatives for this strategy were laid out in the strategy's executive summary:

> 'We live in times of existential crisis, within and beyond the European Union. Our Union is under threat. Our European project, which has brought unprecedented peace, prosperity and democracy, is being questioned. To the east, the European security order has been violated, while terrorism and violence plague North Africa and the Middle East, as well as Europe itself.'[76]

Released in 2016, Mogherini believed that the EUGS was crucial to 'help our Union to re-discover its identity, its soul.'[77] It envisaged a global role for the EU based on 'principled pragmatism'—that is, the EU's engagement in global affairs according to the imperative of resilience and capacity building, in line with EU values and principles.[78] In so doing, it advanced a new, bolder discourse of European 'strategic autonomy', which approached global affairs through a pragmatic, disillusioned orientation.[79] Moreover, the EUGS advanced a vision

---

[75] Johannes Hahn, in Nitoiu and Sus, "Introduction: The Rise of Geopolitics in the EU's Approach in Its Eastern Neighbourhood."

[76] European Union, *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy*, 2.

[77] Federica Mogherini, "Speech by HR/VP Mogherini at the EUISS Annual Conference, Towards an EU Global Strategy-The Final Stage ," April 22, 2016.

[78] Ana E. Juncos, "Resilience as the New EU Foreign Policy Paradigm: A Pragmatist Turn?," *European Security* 26, no. 1 (January 2, 2017): 1–18, https://doi.org/10.1080/09662839.2016.1247809.

[79] European Union, *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy*. European Union.

for the EU to become a 'forward-looking cyber player', through engaging 'in cyber diplomacy and capacity building with our partners and seeking agreements on responsible state behaviour in cyberspace based on existing international law,' to maintain European strategic autonomy.[80]

Beneath this vision, Malksöo argues, was the mission of 'keeping faith of the EU citizens in the continuous relevance of the Union,'[81] thus responding to the EU's self-reflexive insecurities about the merits of a European approach to cyberspace. At the same time, however, the strategy was written with the lessons of the Ukraine and migration crises, together with the shift in transatlantic relations, in mind. The strategy's particular focus upon its Neighbourhood as a priority region was influenced, in large part, by the experiences of the Ukraine and migration crises, both of which had unfolded across its borders and its Southern and Eastern Neighbourhoods. Furthermore, the EUGS' objective of 'credible European defence' incorporated the recognition that further European defence spending was necessary to maintain 'healthy' transatlantic relations with the Trump Administration.[82]

With the 'aspiration to transform rather than simply preserve the existing system', the EUGS advanced an 'integrative' foreign policy strategy through a 'joined up approach'.[83] The necessity of a 'joined-up Union' encompassed the greater incorporation of 'all dimensions of EU external action, security and non-security related.'[84] As a consequence of its new 'joined-up approach', the policy area of cybersecurity was taken under the wing of the EUGS framework.[85] With respect to CCB, the EUGS both formalized and accelerated the cross-dimensional approach to cybersecurity which had commenced after the Ukraine crisis, and reinforced policymakers' strategies of relational and spatial othering. Later in 2016, the

[80] European Union, "Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy," 42.
[81] Mälksoo, "Contemporary Security Policy From the ESS to the EU Global Strategy: External Policy, Internal Purpose," 381.
[82] Mälksoo.
[83] Mogherini, "Speech by HR/VP Mogherini at the EUISS Annual Conference, Towards an EU Global Strategy-The Final Stage."
[84] As quoted in Esther Barbé and Pol Morillas, "Cambridge Review of International Affairs The EU Global Strategy: The Dynamics of a More Politicized and Politically Integrated Foreign Policy," 2019, 762, https://doi.org/10.1080/09557571.2019.1588227.
[85] Barbé and Morillas.

Commission launched an initiative to achieve increased cross-dimensional (internal and external) coordination in the cybersecurity and digital contexts,[86] including CCB programmes, in line with the EUGS' emphasis upon 'the close relationship between internal and external security'.[87] Furthermore, the externalising rationale of EU CCB projects was particularly strengthened with the release of the EUGS, which aimed to foster 'a Union that builds on the success of 70 years of peace,'—for which 'our security at home depends upon peace beyond our borders.'[88] Subsequently, the EUGS became a point of reference for its external, spatialized orientation.[89]

Moreover, the influence of the EUGS had already become clear in 2017, whereupon several key strategic objectives—specifically 'European strategic autonomy' and its associated concept of 'responsibility'—were reproduced in the area of (cyber)security and defence. For instance, the 2017 *Reflection Paper on European Defence* stated that, 'we [Europe] should be able to act alone when necessary. More than ever, Europeans need to take greater responsibility for their own security.'[90] This notion was later reflected by the EU's updated cybersecurity strategy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,* released in September 2017. It stressed the EU's goals to encourage 'due diligence and state responsibility in cyberspace', and for the EU to achieve 'greater resilience and strategic autonomy'.[91] Additionally, it reproduced the EUGS' global outlook through its frequent

[86] General Secretariat of the Council, *Council Conclusions: Mainstreaming Digital Solutions and Technologies in EU Development Policy*, Brussels, 2016.

[87] European Commission and HRVP*, Joint Framework on Countering Hybrid Threats: A European Union Response.*

[88] European Union*, Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy,* 5-7.

[89] For instance, a Commission document noted that, as per the EUGS, the EU's 'internal security depends on external security, including security of its geographical neighbour countries. Cyberspace as a global and, to large extent, borderless domain exacerbates risks and vulnerabilities related to interdependencies between states, economies and stakeholders (both public and private). Thus, in its Global Strategy, the EU presented its commitment to increase its focus on cybersecurity and amongst others to invest in cyber capacity building.' In European Commission*, ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries,* 4.

[90] European Commission, *REFLECTION PAPER ON THE FUTURE OF EUROPEAN DEFENCE*, Brussels, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0315, 7.

[91] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. JOIN(2017) 450 Fina*l, Brussels, 2017, 18.

emphasis on the 'global dimension' to cybersecurity.[92] Alike the EUGS, the experience of the Ukraine crisis (and subsequent events) was also hinted in the 2017 cyber strategy, with its assertion that 'the continuously evolving and deepening threat landscape calls for more action to withstand and deter attacks in the future.'[93]

The concept of 'responsibility' also travelled to the context of CCB, in which it was understood both in terms of responsible behaviour in cyberspace and with regards to the EU taking on a greater leadership role to achieve this objective. Significantly, interviewees asserted that leading CCB globally was the EU's *responsibility*.[94] Indeed, 'we [the EU] were asked also by international partners to take more responsibility of what we do and how we do it'.[95] The 2017 strategy thus positioned the EU as an established *leader* in global cyber capacity building, declaring that, 'since 2013, the EU has been leading on international cybersecurity capacity building and systematically linking these efforts with its development cooperation.'[96] Doing so was seen as important for the EU's *ontological security*: for EU officials, the EU's uptake of further responsibility was necessary in order to be seen as a *credible* cybersecurity actor.[97]

Conclusion: Towards European Sovereignty in Cyberspace

As demonstrated by this chapter, during the 2014-mid 2017 period, the EU experienced several transformative events—most prominently, the Ukraine crisis, but also the migration crisis and relations with the Trump Administration among other events—which encouraged the

[92] Eleven times in total. European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. JOIN(2017) 450 Final*, Brussels, 2017.

[93] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. JOIN(2017) 450 Final*, Brussels, 2017, 3.

[94] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee F, interview by author, virtual (online video), April 15, 2021.

[95] Interviewee A, interview by author, virtual (online video), March 5, 2021.

[96] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. JOIN(2017) 450 Final," 19.

[97] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021.

EU to re-evaluate its conception of its Neighbours and its friends, as well as the global environment itself. This is revealed by policymakers' appropriation of *externalisation* and *spatialization* to the context of cybersecurity (e.g. CCB) following their prominent emergence in the context of the Ukraine crisis and subsequent reinforcement with the experiences of several other security crises during the rest of the period. Collectively, these events influenced the EU's cyber policy development and led to the EU's reconceptualized role in cyberspace with the release of the EUGS.

As I will explore in the next chapter, the EUGS laid important groundwork for the emergence of sovereignty discourses in cyberspace and the legitimization of geopolitical language in official EU policy. The progressive entanglement of cybersecurity within the framework of the EUGS facilitated the uptake of particular EUGS ideas and concepts in cybersecurity policy in the late 2017-2020 period, which enabled the adoption of 'sovereignty' in cyber policy discourse. The 2017 *Reflection Paper on the Future of European Defence* (in which cybersecurity was a key priority) foreshadowed this development, noting that further cooperation at the EU level and an enhanced role for the EU would strengthen Member States and make them 'more sovereign.'[98] At the same time, transformative events over the late 2017-2020 period encouraged EU policymakers to recognize the geopolitical dimension in cyberspace, leading to the legitimization of geopolitics in official discourses. It is to this period in time that I will now turn.

[98] European Commission, *REFLECTION PAPER ON THE FUTURE OF EUROPEAN DEFENCE*,11.

Chapter VI – Legitimization and European Sovereignty

This chapter argues that EU cybersecurity policy during the late 2017-2020 period has been characterized by two significant developments: first, Brussels' increased awareness and receptivity to geopolitical concepts, and second, the EU's adoption of sovereigntist discourse to position itself as a cyber actor**,** whereby it has begun to 'speak in geopolitical terms.' This contemporary phase of the EU's cyber policy development marks the culmination of EU policymakers' efforts to manage insecurities in cyberspace and envision a role for the EU.

This chapter documents how transformative events in the cyber environment spurred EU policymakers to recognize the 'geopolitical dimension' to cyberspace, which led to the emergence of geopolitical language in official EU discourses. Specifically, global security disputes over Chinese state-sponsored 5G networks beginning in 2018 and the threat of weaponizing interdependencies in cyberspace (especially during 2020) were perceived by EU policymakers as irrefutable evidence of geopolitical activities in cyberspace, leading to their recognition of the 'geopolitical dimension'. Furthermore, the recently elected Biden Administration encouraged EU officials and experts to more deeply consider geopolitical dynamics in cyberspace, which helped to legitimize geopolitical discussions in an official EU capacity. Despite the EU's transition to speaking 'in geopolitical terms', EU officials continued to distance the EU from geopolitical actors when representing the EU's identity. In so doing, the EU's enduring autobiographical insecurity about geopolitics incorporated a new *relational* dimension.

Simultaneously, these transformative events emphasized to Brussels that the EU should take greater responsibility in cyberspace and seek to alleviate Europe's dependency on other actors. These beliefs helped to bring about the conceptual appropriation of 'European sovereignty' from the EUGS framework to the cyber context. Moreover, EU officials' insecurities about the EU's association with geopolitics were instrumental for the emergence

of 'European sovereignty' as a *main objective* in EU cyber policy, and these anxieties continued to influence how policymakers constructed the EU's role as a cyber actor during this period of time. The invocation of 'European sovereignty' to construct the EU's role in cyberspace, however, has remained subject to internal contestation and conceptual disagreement.

From Awareness to Action

By the end of 2017, the EU was disillusioned by its global environment—security crises in 2014, 2015, and Trump's election in 2016 had brought about the impression that the EU was surrounded by a 'ring of fire', as the previous chapter revealed. This revelation opened up the door for geopolitically oriented discussions at the EU level between Member States about the question of how to increase Europe's strategic autonomy in the increasingly inhospitable global environment. France, for one, believed that 'we aren't big enough and strong enough by ourselves and therefore, this [security] is something that we should be doing at the European level.'[1]

As a first step, some Member States turned to capabilities-based solutions and advocated for increasing the EU's security capabilities.[2] This idea was later reproduced in the Council's *Reflection Paper on the Future of European Defence* (2017), in which the EU was conceived as a 'continental-sized power', 'far better equipped than small-to-medium sized states'—thus drawing upon the geopolitical logic of 'power multiplier.'[3] Indeed, the EU's 2017 cybersecurity strategy voiced the need for the EU to increase its capabilities in intelligence-gathering and cyber-technologies—material capabilities often associated with traditional geopolitical thinking.[4] In addition to technological assets, data was understood as a key

[1] Interviewee C, interview by author, virtual (online video), March 12, 2021.

[2] Interviewee C, interview by author, virtual (online video), March 12, 2021

[3] Aharon Klieman, *Great Powers and Geopolitics: International Affairs in a Rebalancing World* (Springer Press, 2015), http://www.springer.com/series/10201.

[4] As argued in Chapter 2; see also Cai, "Geopolitics in the Cyberspace: A New Perspective on U.S.-China Relations."

resource in this regard. As one EU official reasoned, 'the more the more data you have, the better technology [you] can develop' making it a 'question of critical mass' in the context of technological leadership (Interviewee E, 2021).[5] Later, the imperative to strengthen the EU's industrial and technological capabilities was emphasized by the EU's most recent 2020 global strategy, *Shaping Europe's Digital Future,* in order to 'advance the European approach' to cyberspace.[6]

Below, I explore how several developments in cyberspace—namely 5G networks, weaponizing interdependencies, and a reorientation in transatlantic relations—were transformative for the EU's particular 'worldview' in the context of cyberspace. The collective experience of such critical events—particularly their destabilizing effect upon the EU's ontological security—led to the EU's reconceptualization of cyberspace to become more inclusive of geopolitical considerations. This awareness was accompanied with an accelerated sense of urgency, given that cybersecurity risks were 'increasing' and deepening 'exponentially.'[7]

Diktat Anxieties (5G), Weaponizing Interdependencies, and Transatlantic Implications

Rising security concerns about 5G networks, particularly their connection to Chinese cyber espionage and related security risks, were a critical 'wakeup call' to EU policymakers.[8] 5G networks facilitate the 'Internet of Things' through connecting key domains—including political, strategic, military, economic, industrial dimensions—at the personal, local, national,

[5] Interviewee E, interview by author, virtual (online video), March 25, 2021.

[6] European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Shaping Europe's Digital Future*, Brussels, 2020.

[7] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. JOIN(2017)* ; Final, Brussels, 2017, 2.

[8] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

and international levels.[9] Thus, 5G 'high capacity' networks have been crucial for enabling the EU to compete in the global market, as they support 'new types of applications connecting devices and objects', and the virtualisation of multiple sectors: transport, health, manufacturing, energy, media, logistics, and entertainment.[10] Figure 6 visualizes the Commission's conception of 'What 5G is about.'



Figure 6. EU Commission diagram on 'What 5G is about' (2020). [11]

Indeed, while the EU has been formally pursuing 5G through research and development projects since 2013,[12] security concerns explain why 10 Member States have yet to implement 5G networks into their critical services (as of the end of 2020).[13] These security concerns rose to the fore after the US banned 5G technology supplied by Huawei, the Chinese telecommunications company, accusing it of state-backed cyber espionage. Amongst the national security issues raised by Washington were concerns about 'digital backdoors', intellectual property theft, and the company's obligation to adhere to Chinese data and

[9] Samuele Dominioni and Fabio Rugge, "THE GEOPOLITICS OF 5G ," September 2020, https://www.ispionline.it/sites/default/files/pubblicazioni/dossier_cyber_5g_september_2020.pdf.

[10] European Commission (SWD), "Staff Working Document: 5G for Europe: An Action Plan 2016 Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions Brussels," 2016, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131.

[11] European Commission, *5G Action Plan : Shaping Europe's Digital Future,* Brussels, March 9, 2021, https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan.

[12] European Commission, "Action Plan 5G for Europe2016 - Staff Working Document," 2016.

[13] European Court of Auditors, "Audit Preview: Implementing Secure 5G Networks in the EU and Its Member States," 2020.

intelligence sharing laws.[14] Particularly, concerns about China's 2017 *National Intelligence Law*, which obliged enterprises to cooperate with Chinese intelligence authorities,[15] brought about the decision to ban Huawei by several other Western countries, including Australia and Japan.[16] For the EU's part, 'enhancing the cybersecurity of the Union' became a Commission priority in 2019, whereupon it recognized the significance of 5G networks and the widening 'attack surface' of such networks.[17] After conducting a coordinated risk assessment,[18] the EU adopted its '5G Toolbox' for cybersecurity in 2020.[19]

Moreover, the Huawei '5G' case demonstrated to EU officials the 'increasing entanglement' of power politics between states and *digital geopolitics*.[20] For EU policymakers, it also triggered the unavoidable realization that instabilities in global cyberspace mirror insecurities in other political domains, particularly China's 'rise' in the global system.[21] Given that the world's leading companies in 5G have been Chinese state-backed firms, China has been highly influential in shaping international standards for the 5G market.[22] China's rising technological superiority in cyberspace, particularly in light of its rapidly expanding Belt and Road Initiative, has fuelled perceptions (from both policymakers and scholars alike)[23] that there is an unfolding 'digital' or 'cyber' geopolitical competition between US and China. As one interviewee (Interviewee E) recalled, Chinese strategies towards 5G network funding and

[14] European Parliament, "Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them," 2019.

[15] Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant ," Council on Foreign Relations, August 6, 2020, https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

[16] Maizland and Chatzky.

[17] European Commission*, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Twentieth Progress Report towards an Effective and Genuine Security Union,* Official Journal of the European Union, Brussels, 2019.

[18] NIS Cooperation Group, "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks," *European Commission*, 2019, https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

[19] European Commission, "Secure 5G Networks : Questions and Answers on the EU Toolbox," no. January (2020), https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

[20] Annegret Bendiek, Nadine Godehart, and David Schulze, "Global: The Age of Digital Geopolitics ," *International Politics and Society*, 2019, https://www.ips-journal.eu/regions/global/the-age-of-digital-geopolitics-3593/.

[21] Interviewee D, interview by author, virtual (online video), March 18, 2021.

[22] Luca Tarantino, "The 5G Moment of Truth in Europe: Geopolitical Implications, Economic Opportunities and Cybersecurity Concerns," 2020.

[23] As reviewed in Chapter 2. See for example Weber, "Making Sense of Technological Spheres of Influence"; Tarantino, "The 5G Moment of Truth in Europe: Geopolitical Implications, Economic Opportunities and Cybersecurity Concerns"; Shawn M. Powers and Michael Joblanski, *The Real Cyber War : The Political Economy of Internet Freedom*, 2015, https://ebookcentral.proquest.com/lib/oxford/detail.action?docID=3414433.

development 'is not done in isolation, but that is part and parcel of a strategy of […] technological leadership.'[24] Beyond intelligence and data sharing concerns, the economic and technological dominance of Chinese companies in the EU's 5G market has raised worries about the lack of a level playing field in European industry.[25] Overall, the '5G dispute' brought about a more fundamental realization for EU policymakers: that there was an unfolding systemic geopolitical shift in cyberspace.

The EU's newfound geopolitical awareness is evinced by its 2019 *EU-China* strategic outlook document. It referred to China as both a partner and *a systemic rival*, demonstrating a clear shift in orientation in EU-China bilateral relations to incorporate the issue of geopolitical competition.[26] Additionally, in March 2019 the European Parliament published a dedicated resolution on '*Security threats connected with the rising Chinese technological presence in the EU'*.[27] It noted that non-EU 5G vendors could pose security risks to the EU due to laws in their country of origin—particularly the Chinese State Security Laws—and the need for a 'thorough investigation' about whether the devices or suppliers present risks to the EU's security. [28] This was later reiterated in a broader sense within the Commission's progress report on *the Security Union* in October 2019, which noted the importance of the 'risk profile of individual suppliers', which would be determined in part by the 'likelihood of the supplier being subject to interference from a non-EU country.'[29] As Chinese companies comprise a large portion of shares in the European telecommunications market and enjoy better (Chinese state-funded) subsidies compared to their European counterparts, concerns have been raised about foreign

[24] Interviewee E, interview by author, virtual (online video), March 25, 2021.

[25] Interviewee A, interview by author, virtual (online video), March 5, 2021. Also: Council of the European Union, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Establishing the European Defence Industrial Development Programme Aiming at Supporting the Competitiveness and Innovation Capacity of the Union's Defence Industry* SN 2717/18, no. July 2018, Brussels, 2018: 1–37.

[26] European Court of Auditors, "The EU's Response to China's State-Driven Investment Strategy," no. 0 (2020).

[27] European Parliament, "Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them."

[28] European Parliament.

[29] European Commission, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Twentieth Progress Report towards an Effective and Genuine Security Union,* 8.

direct investment in 5G and other digital technologies.[30] Security disputes over 5G have also driven EU policymakers to identify cyber espionage (as distinct from disruptive cyberattacks) as a significant emergent threat in cyberspace.[31] In this regard, the EU has officially acknowledged that cyberespionage through 5G networks is likely to be posed by 'state or state-backed actor[s],' particularly levelling its attention to the Chinese state-backed companies Huawei and ZTE.[32]

Thus, the '5G' phenomenon, especially in the context of rising Chinese technological superiority and international influence, was particularly consequential for EU policymakers' concerns about dependency in cyberspace. Whereas such concerns had been largely centered around the issue of the EU's dependency on foreign technology and thus foreign (private/corporate) suppliers in earlier years, there was now a more pronounced, urgent concern that Europe could become subject to the *(geo)political* motives of foreign *state* actors. Particularly, policymakers realized after the 5G dispute that geopolitical aspects have become intertwined and interdependent with economic considerations.[33] Accordingly, the relationship between finance and security in cyberspace has emerged as a 'big priority' in COREPER I discussions, with a focus on how technology affects both the internal market *and* foreign affairs, particularly countries' relationships with China.[34] Discussing this, EU officials articulated concerns about being 'deadlocked with one country'[35] (Interviewee A) and therefore subjected to the dictates of that state.[36] This can be understood as anxiety about *diktat* in cyberspace, or the external imposition of fundamental rules of governance and daily life without popular consent. Indeed, these concerns motivated the European Parliament's call for

[30] European Commission, *Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Proposal for a Regulation of the European Parliament and of the Council. COM(2018) 630 Final.*

[31] Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021.

[32] NIS Cooperation Group, "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks."

[33] Interviewee B, interview by author, virtual (online video), March 11, 2021.

[34] Interviewee B, interview by author, virtual (online video), March 11, 2021.

[35] Interviewee A, interview by author, virtual (online video), March 5, 2021.

[36] Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

'the Commission to develop a strategy that puts Europe in a leading position in cybersecurity technology'—one that is 'aimed at reducing Europe's dependency on foreign technology in the field of cybersecurity'[37] and premised upon EU democracies.[38]

However, the anxiety about foreign *diktat* was not the only looming concern for EU policymakers. A second prominent development raised by interviewees during 2018-2020 period was the EU's rising awareness that interdependencies can be weaponized in cyberspace,[39] as it is understood that 'those who pioneer certain technologies will have a stronger influence in the future' (Interviewee E, 2021).[40] This strategy is leveraged by powerful states within asymmetrical network structures, which can use 'interdependent relations to coerce others' to fulfil their strategic aims.[41] In 2018, European concerns about this tactic were exacerbated after President Trump withdrew from the Joint Comprehensive Plan of Action Agreement to impose sanctions on Iran, which caused significant global economic and financial consequences, including in Europe.[42]

By the outbreak of the COVID-19 pandemic (beginning in March 2020),[43] EU officials had observed with increasing unease that cyber actors had 'weaponized interdependencies' in supply chains 'to get an edge in the [global geopolitical] competition' (Interviewee E, 2021).[44] For instance, they noted that the US had adopted this strategy in effort to curtail the influence of Huawei.[45] Moreover, weaponized interdependencies were starkly evident during the ongoing COVID-19 pandemic, which was fraught with supply chain issues and cyberattacks. This threat was particularly grave, as the EU—and the rest of the world—had become even

[37] European Parliament, "Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them."

[38] Interviewee E, interview by author, virtual (online video), March 25, 2021.

[39] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

[40] Interviewee E, interview by author, virtual (online video), March 25, 2021.

[41] Adam Segal, "Huawei, 5G and Weaponized Interdependence," in *The Uses and Abuses of Weaponized Interdependence*, ed. Daniel W. Drezner, Henry Farrell, and Abraham L. Newman (Brookings Institution Press, 2021).

[42] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 45, https://doi.org/10.1162/ISEC_a_00351.

[43] COVID-19 was declared to reach 'pandemic status' in March 11, 2020, by the World Health Organization. "A Timeline of COVID 19 Developments in 2020," American Journal of Managed Care, January 1, 2021, https://doi.org/10.1200/JCO.20.02608..

[44] Interviewee E, interview by author, virtual (online video), March 25, 2021

[45] Segal, "Huawei, 5G and Weaponized Interdependence."

more dependent on digital technologies for the basic necessities of life, including financial and physical wellbeing.[46] Thus, the pandemic was regarded by EU officials not only as an 'accelerator of existing trends' but as fundamentally changing European life, including how 'we understand and implement foreign policy' (HRVP Borrell, 2020).[47] Thus, the Council Conclusions of June 2020 stressed 'protecting and reinforcing digital sovereignty in the EU and leadership in strategic international digital value chains as key elements to ensure strategic autonomy, global competitiveness and sustainable development.'[48]

Finally, alongside 5G 'digital geopolitics' concerns and the weaponization of interdependencies, the shift in transatlantic relations after the election of US President Joe Biden in November 2020 was particularly significant for encouraging European policymakers to further consider and engage with the geopolitical and security consequences of cyberspace, particularly in terms of transatlantic cooperation.[49] An interviewed EUISS policy expert noted that from 2020 onwards, the 'US has reached out a lot more to Europeans to work with Europeans on tech topics,' which was motivated by American intentions to form a 'common front against China' (Interviewee C, 2021).[50] As part of her professional experience, she recently witnessed the State Department's invitation of European AI experts to engage in discussions about technology, which brought about the European realisation that AI is a topic for international cooperation on geopolitics (Interviewee C, 2021).[51] It was through these types of interactions, she argues—in addition to 5G concerns—that Europeans were 'woken up' to the geopolitical aspects of security in cyberspace.[52] At the same time, Washington's encouragement for the EU to consider the geopolitical dimension to cyberspace contributed to

[46] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.
[47] As interviewed by Weiler, "Europe Must Learn Quickly to Speak the Language of Power."
[48] General Secretariat of the Council, *Shaping Europe's Digital Future - Council Conclusions*, Brussels, 2020, 4.
[49] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021.
[50] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[51] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[52] Interviewee C, interview by author, virtual (online video), March 12, 2021.

the concept's normalization within EU policy discourses, as it signalled that a key ally accepted the EU speaking in 'geopolitical terms'.

As a consequence, one EU official noted that, 'as we see how the discussions are developing, it's not only technical issues, they are very much about the geopolitics' (Interviewee A, 2021).[53] Two significant developments resulted from the 5G 'wakeup call' according to another EU policymaker: the first development being the EU's repositioning as a 'welcome player' in dealing with European cybersecurity issues in the eyes of Member States, and secondly, it became 'obvious' to officials that cyberspace would be the 'most noticeable' site in which the unfolding geopolitical competition between major global players would take place (Interviewee E, 2021).[54] The sense that there was a 'greater acceptance' of the EU engaging in geopolitical thinking was similarly expressed by an interviewed EUISS policy expert (Interviewee C, 2021).[55]

The EU's transition to speaking in geopolitical terms could not have been made clearer in September 2020, when HRVP Josep Borrell officially emphasized 'that cyber issues are geo-political in nature and have a strong security dimension,' at the EU Cyber Forum.[56] Taking a 'geopolitical perspective', Borrell outlined five defining features of 'today's arena': the current 'unprecedented competition between states' as a 'world of power politics'; the 'paralysing' global effect of strategic US-China competition which has led to increasing global dissensus; the issue of weaponised interdependencies; a trend 'where some countries seem to follow a logic of empires'—in which they argue 'in terms of zones of influence'; and the ongoing 'battle of narratives' in the digital domain.[57] As part of this broader awareness of the 'geopolitical', dependency anxieties took on an additional geopolitical dimension during this period. [58] The

[53] Interviewee A, interview by author, virtual (online video), March 5, 2021
[54] Interviewee E, interview by author, virtual (online video), March 25, 2021.
[55] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[56] Josep Borrell, "Cyber Diplomacy and Shifting Geopolitical Landscapes," 2020.
[57] Josep Borrell, "Cyber Diplomacy and Shifting Geopolitical Landscapes," 2020.
[58] Interviewee C, interview by author, virtual (online video), March 12, 2021.

sense of 'falling behind' pervaded this geopolitical awareness, as EU policymakers felt that there were 'different areas where we, I don't want to say that we were slipping, but in which we have to catch up,' (Interviewee A, 2021).[59] At this 'geopolitical hour', therefore, EU officials realized that the EU had secure Europe's digital sovereignty before it was too late.[60]

The Emergence of Sovereignty in EU Cybersecurity Policy

Whereas the EU had previously emphasized Member States' *sovereignty*—or indeed *sovereignties*—in its foreign policy and security discourses,[61] this terminology was largely replaced by the concept of 'European sovereignty' in the contemporary period. By 2018, the necessity that '*Europe* has to be a more sovereign *actor*' was asserted by then-Commission President Juncker, and in 2019, the singular notion of 'European sovereignty' became a 'major objective' in EU policies, such as the *Commission Recommendation on the Cybersecurity of 5G Networks.*[62] 'European sovereignty' in the digital context was also centrally featured within Von der Leyen's Commission Presidency platform and carried forward as a priority following her election in 2019.[63]

The emergence of European sovereignty in the cybersecurity context can be explained in part by the progressive integration of cyber policy with the EU's broader global strategic outlook over time. As briefly mentioned in the previous chapter (V), ideational convergence between the EUGS and cyber discourse had proceeded with the concepts of 'responsibility' and 'strategic autonomy' travelling to the cyber context, after the EUGS (2016) and the Commission had stressed that it was time Europeans took 'greater responsibility for their own

[59] Interviewee A, interview by author, virtual (online video), March 5, 2021

[60] Jean-Claude Juncker, "State of the Union 2018: The Hour of European Sovereignty," European Commission, 2018, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en_0.pdf.

[61] For instance, the 2017 *Reflection Paper on the Future of European Defence* asserted the imperative to have 'stronger and *more sovereign Member States*' in order to establish a security and defence Union.

[62] European Commission, *COMMISSION RECOMMENDATION of 26.3.2019 Cybersecurity of 5G Networks,* Brussels, 2019, https://doi.org/10.4018/978-1-7998-7708-0.ch029.

[63] Ursula Von der Leyen, "Political Guidelines for the next European Commission, 2019-2024," 2020, https://doi.org/10.5771/2193-5505-2020-3-253.

security.'[64] By 2018, EU discourses had established an overt link between the ideas of *European sovereignty, leadership* and *autonomy* to EU cybersecurity policy, particularly with regards to the EU's objectives and ambitions in cyberspace *(visualized in Appendix 3).* Responsibility was cited by one EEAS official as the primary reason for the emergence of European digital sovereignty in the first instance: simply, 'we were asked also by international partners to take more responsibility of what we do and how we do it.'[65] Alternately, an EUISS policy expert noted that, over time, the 'tech theme became important' in general discussions regarding European strategic autonomy between Member States, which precipitated the emergence of this 'kind of European digital sovereignty' concept.[66]

Ideational convergence along these lines is further exemplified by how EU policymakers explained the EU's *earlier* external actions in cyberspace (before the concept was officially introduced) on the basis of 'European sovereignty.' Indeed, an EU official noted that European digital sovereignty was 'already an explanation [for] how we understand this…international aspect,' (Interviewee A, 2021).[67] They asserted that the concept of multilateralism was 'binded [sic] together' with sovereignty, as sovereignty entailed the EU taking more responsibility and engaging with third countries (Interviewee A, 2021).[68] The connection between multilateralism and sovereignty was echoed by another EU official, albeit from a slightly different perspective. They stated that, 'The idea [of sovereignty] is key in the sense that what we mean by digital sovereignty is sovereignty, the ability to decide', including the capacity to decide between multiple suppliers in a multilateral setting (Interviewee E, 2021).[69]

[64] European Commission, *REFLECTION PAPER ON THE FUTURE OF EUROPEAN DEFENCE,* 2017, 11.
[65] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[66] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[67] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[68] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[69] Interviewee E, interview by author, virtual (online video), March 25, 2021.

It is also traceable through textual linkages between 'sovereignty', 'responsibility', and 'leadership', whereby EU documents have constructed the EU as assuming its rightful, credible, and necessary role in cyberspace. This coheres with the EUGS assertion that 'the EU will be guided by a strong sense of responsibility'[70] later expressed by Commission President Juncker, who declared that 'it [was] time Europe took its destiny into its own hands.'[71] The importance for the EU to take the lead in preserving *European* sovereignty was further reiterated by the EU Commission's Recommendation on the *Cybersecurity of 5G Networks* in 2019, which asserted that 'ensuring European sovereignty should be a major objective' for the EU, particularly given the security risk posed by foreign investment in strategic sectors and foreign technologies and critical infrastructures in the Union.[72] That same year, the European Parliament asserted that the Union must 'take the lead on cybersecurity' and that the Commission must develop a strategy in which Europe has a 'leading position' in cybersecurity technology.[73] Accordingly, the EU's *Strategic Outlook* on China asserted that the EU 'should foster industrial cross border cooperation, with strong European players, around strategic value chains that are key to EU industrial competitiveness and *strategic autonomy.*'[74] Subsequently, the EU's 2020 strategy, *Shaping Europe's Digital Future,* advanced the reasoning that, 'the European model has proved to be an *inspiration* for many other partners around the world as they seek to address policy challenges, and this should be no different when it comes to digital.'[75] Thus, the EU's historical position of technological leadership, and the success of the 'European model' has been advanced as the justification for taking a more assertive, and distinctively *European* approach to cyberspace and digital affairs.

---

[70] European Union*, Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy, 8.*

[71] Juncker, "State of the Union 2018: The Hour of European Sovereignty," 5.

[72] European Commission*, COMMISSION RECOMMENDATION of 26.3.2019 Cybersecurity of 5G Networks.*

[73] European Parliament, "Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them."

[74] European Commission and HRVP, *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL EU-China – A Strategic Outlook*, Brussels, 2019, 8.

[75] Emphasis added. General Secretariat of the Council, *Shaping Europe's Digital Future - Council Conclusions*, 13.

European Sovereignty as a Form of Differentiation

While cyber policy's integration with foreign and security policy explains the transference of 'European sovereignty' to the cyber context, it cannot sufficiently explain why the concept rose to prominence above other key ideas, such as 'European leadership' or 'European autonomy' to become one of the most prominent catchphrases in the current Von der Leyen/Borrell 'geopolitical commission'. I argue that ontological motives are important for explaining why European sovereignty reached such a *prominent position* in EU cyber policy discourse over time, from its feature in Von der Leyen's Presidential platform to becoming the 'vision' for Europe's digital future in 2020. Exploring how European sovereignty has emerged in parallel with geopolitical language within EU cybersecurity policy reveals this particular dynamic. Specifically, policymakers' ontological insecurities about 'speaking in geopolitical terms' created the impetus for the EU to differentiate itself from geopolitical others through the language of 'European sovereignty'.

The Spectre of Geopolitics

As argued in Chapter III, the EU's eschewal of geopolitics in the context of its own policymaking has been a longstanding discursive trend,[76] and it is closely tied together with the EU's 'founding myth' for its political existence. Thus, it is conceivable that the transition to openly taking a 'geopolitical perspective' would elicit anxieties reconciling the EU's historical self-representation as non-geopolitical and the current 'geopolitical commission' in Brussels. Interviewee responses indicate such insecurities, suggesting that, while geopolitical conversations had become normalized and even encouraged by the late 2017-2020 period by the EU's allies (with the President Biden's election), the capacity to 'speak in geopolitical

[76] See also: David Cadier, "The Geopoliticisation of the EU's Eastern Partnership," *Geopolitics* 24, no. 1 (2019): 71–99, https://doi.org/10.1080/14650045.2018.1477754; Diez, "Europe's Others and the Return of Geopolitics."

terms' has been constrained by enduring cultural expectations (and anxieties) about the EU's self-representation as a non-geopolitical actor. Particularly, interviewees' frequent[77] reliance upon relational othering suggests enduring anxieties about the EU engaging with geopolitical concepts, yet an externalised, rather than self-reflexive, locus of such insecurity. Instead of framing such insecurities relative to a temporal other (e.g. its past Self), interviewees consistently defined the EU's role in cyberspace relative to other contemporaneous geopolitical actors. Relational othering consistently arose during conversations about the EU's CCB projects and regarding the EU's goals and priorities in cyberspace, whereby interviewees emphasized how important it was that I did not misunderstand the EU's approach to cyberspace.

With regards to the EU's CCB projects in Africa, interviewees were at pains to clarify that the EU was 'not engaging in geopolitical battles' (Interviewee E, 2021),[78] and its development projects were *not* carried out in a geopolitical way.[79] Indeed, EU officials were adamant that Europe's intentions with such programmes should not be misunderstood as protectionist or geopolitical. They were dismayed that 'some colleagues' and 'some others' had questioned Europe's attempts to 'create an island and to separate [itself]' when it 'does not have capability to do it' (Interviewee A, 2021).[80] On the contrary, the EU has moved towards reducing barriers and creating opportunities, as opposed to erecting borders, another official told me.[81] Separately, an EUISS policy expert confirmed that this 'island of Europe' issue was raised in Washington. However, she believed that the Americans never took this possibility seriously; instead, 'we definitely thought about this more in Berlin and Warsaw than they ever did in DC' (Interviewee C, 2021).[82] In other words, concerns about the EU becoming

[77] Indeed, all interviewed *EU* officials (4 total) and one cyber policy expert (employed in an affiliated think tank) engaged in this strategy. Interviewees A, B, C, D, respectively (2021). *See appendix 3.2 for further examples.*

[78] Interviewee E, interview by author, virtual (online video), March 25, 2021.

[79] Interviewee E, interview by author, virtual (online video), March 25, 2021; Interviewee A, interview by author, virtual (online video), March 5, 2021.

[80] Interviewee A, interview by author, virtual (online video), March 5, 2021.

[81] Interviewee B, interview by author, virtual (online video), March 11, 2021.

[82] Interviewee C, interview by author, virtual (online video), March 12, 2021

geopolitical were largely concentrated *within* EU Member States and/or EU contexts as opposed to in Washington or other EU allies. Thus, it appears that there remains a strong, *internally driven* anxiety about the EU's self-positioning vis-à-vis geopolitics, and the EU's socio-historical background has constrained its usage.

Notably, the issue that I could 'misrepresent' or 'misunderstand' the EU's role in global cyberspace was a consistent and highly sensitive issue during our conversations.[83] For these interviewees, it was imperative that I *correctly* understood the EU's position and goals relative to others in cyberspace. To explain the EU's intentions in cyberspace, interviewees frequently contrasted the EU with what were considered to be 'traditional' (Westphalian) geopolitical actors: China, Russia, and the US. Indeed, interviewees described the EU as post-Westphalian insofar as it lacked the trappings—and competences—of nation states in the area of security.[84] This contrast helped to establish that, beyond the EU's preference to eschew geopolitics, the EU was *incapable* of engaging geopolitically in the same manner as other actors.[85] Specific to cyberspace, the EU's 'different-ness' from Westphalian actors was positively framed as endowing the EU with 'neutral status' (Interviewee A, 2021), which was seen as an asset in the ongoing geopolitical competition in cyberspace—whereas other actors, namely the US and China, were clearly *not* neutral.[86]

Additionally, interviewees linked the EU's approach to CCB projects with the ideas of openness, empowerment and co-ownership[87] and collectively stressed the EU's goals of providing a 'fair' and 'level playing field' for third countries.[88] These virtues were directly

[83] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

[84] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee F, interview by author, virtual (online video), April 15, 2021.

[85] Interviewee C, interview by author, virtual (online video), March 12, 2021.

[86] Interviewee A, interview by author.

[87] Interviewee A, interview by author; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee C, interview by author, virtual (online video), March 12, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

[88] Interviewee A, interview by author; Interviewee D, interview by author, virtual (online video), March 18, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.

juxtaposed with Russian and Chinese projects, which were described as dictatorial, unequal, geopolitical, and entailing the sole ownership by Russia or China of third countries' infrastructure and data. Thus, the EU's CCB programmes were described as providing 'freedom of choice' as opposed to Russian and Chinese projects, which subjected third countries to dependency and dictation.[89] Whereas Russia and China's cyber capacity building projects were described as putting African countries in a position of dependence, interviewees took care to contrast this with the EU's approach as 'ready to help and not to buy you [like China and Russia]' (Interviewee A, 2021).[90] Unlike the Russian and Chinese *asymmetric* development projects, therefore, officials stressed that the EU's approach has been guided by the principle of multilateralism and universal values, in which the EU and its third country partner 'co-own' the CCB project (Interviewee A, 2021; Interview E, 2021).[91]

In sum, interviewees generally distinguished between 1) the EU and 'traditional' geopolitical actors, such as the US, China, and Russia, and 2) the EU and those seeking to cordon global cyberspace in a 'protectionist' and 'conflictual' manner (viz. China and Russia). In doing so, interviewees' narrative constructions of the EU's identity as a cybersecurity actor drew both on its existing successes in development and peace projects, which were juxtaposed by its 'separateness' from geopolitical actors such as the US, China, and Russia (*see Appendix 3.2 for further examples*). On the basis of textual sources and interview responses, it is possible to develop a visual representation of this othering strategy, in line with Derrida's method of deconstruction (Figure 7).

[89] Interviewee A, interview by author; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee E, interview by author, virtual (online video), March 25, 2021.
[90] Interviewee A, interview by author.
[91] Interviewee A, interview by author; Interviewee E, interview by author, virtual (online video), March 25, 2021.

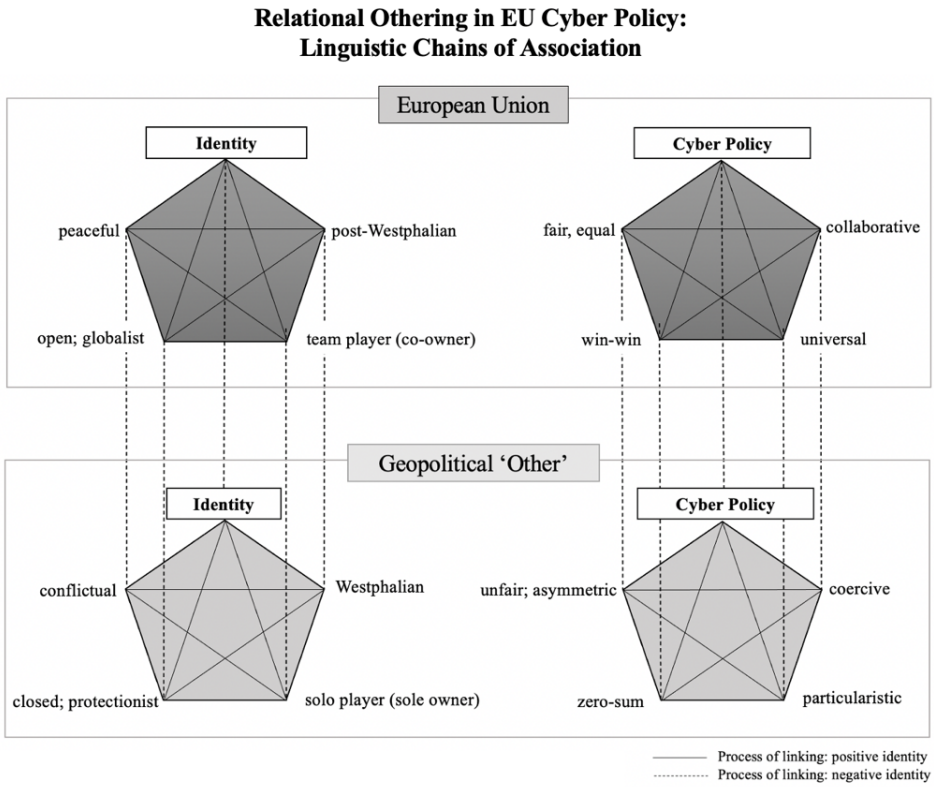


Figure 7. Relational Othering in EU cyber policy discourse.

As interviewees' concerns about misrepresentation suggest, the EU's embrace of geopolitical language has come into tension with its autobiographical insecurities associated with the EU's geopolitical past. Furthermore, it suggests that the EU's embrace of geopolitical language aroused further anxieties about the EU's construction as a cyber actor, as it introduced the possibility that the EU could be *misunderstood by others* as a geopolitical actor. Overall, this reveals that, while the EU's 2020 global strategy claims that 'European sovereignty is not defined against anyone else,' EU policymakers have relied upon this concept to differentiate the EU from 'geopolitical competitors' in cyberspace, in order to construct the EU's identity in a way that is culturally and politically coherent with the EU's notion of Self.

Responding to Geopolitics with European Sovereignty

Furthermore, the EU's calls for 'healthy competition' in cyberspace is a particularly illustrative example of how EU policymakers have drawn upon European sovereignty to

negotiate insecurities about being construed as a geopolitical actor. In response to the increased presence of foreign technological actors (including China) in its Internal Market, European policymakers have emphasized the importance of 'healthy [economic] competition' in cyberspace and the need to 'keep up' with 'frontrunners' (Interviews 1 and 2, 2021). 'Healthy competition' encompasses the idea of ensuring a 'level playing field' for economic actors in cyberspace. It pays homage to the EU's long tradition of incorporating liberal market economic logics into its policies, as well as its self-representation as a fair economic player. At the same time, however, the discourse has established a relational distance from other actors, whose economic development projects have been described as 'zero-sum'. By contrast, the EU's aim of 'healthy competition' has been framed as a 'win-win' situation for the EU and its partners—hence the emphasis on *healthy*.[92]

In this policy context, 'European sovereignty' has emerged as an additional strategy to differentiate the EU from other geopolitical actors through the concept's construction as inextricably tied to the EU's economic security. Former EU Commission President Juncker articulated this logic in his 2018 *State of the Union* speech, arguing that rather than militarization and protectionism, 'the Euro must become the face and the instrument of a new, more sovereign Europe.'[93] Leveraging the economic assets of the EU for the current 'geopolitical hour'[94] emphasizes the EU's material (economic) capabilities as significant for its positioning in a geopolitical context. Similarly, an interviewee noted the importance of 'helping develop competitive solutions' to ensure European sovereignty (Interviewee E, 2021).[95] Accordingly, the EU's industrial 2018 strategy emphasizes 'made in Europe' solutions and the further regulation of foreign direct investment as essential to create 'a level playing

[92] European Commission, "COMMISSION STAFF WORKING DOCUMENT Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy" (Brussels, 2017), 15. Also: Interviewee A, interview by author, virtual (online video), March 5, 2021.

[93] Juncker, "State of the Union 2018: The Hour of European Sovereignty."

[94] Juncker.

[95] Interviewee E, interview by author, virtual (online video), March 25, 2021.

field',[96] which was later reiterated by the EU's 2020 *Industrial Strategy for Europe* as necessary for European sovereignty.[97] The current transition in digital leadership, it asserted, was a crucial time for 'Europe to affirm its voice, uphold its values and fight for a level playing field…this is about Europe's sovereignty'.[98] More broadly, the objective of European sovereignty has geopolitical benefits: European investment in 5G technologies was seen as necessary 'in order to be a credible partner for the others [external partners]' and 'to have a serious discussion later on with the big powers like China, us or Russia, otherwise, we will be left behind […]' (Interviewee A, 2021).[99]

Overall, it appears that 'European sovereignty' has been aimed at mitigating the potential misconception—and relational insecurity—that the EU has become a geopolitical player in cyberspace. Adopting the language of 'sovereignty' and 'responsibility' to explain the EU (and Europe's) increased role in cyberspace constructs Europe as taking up its *rightful* place in cyberspace and asserting its *sovereign, legitimate* authority to ensure the future of European existence in global cyberspace. Thus, to achieve this sovereignty, Europe 'needs to be a strong, independent and purposeful digital player i*n its own right.*'[100] In the perspectives of policymakers, therefore, 'European digital sovereignty' has entailed the assertion of control over space and entities that were already—and have always been—legitimately European. The concept of 'sovereignty' therefore also seeks to convey what the EU is *not.* It is *not* exerting authority over space or entities seized from another political actor (which are, by definition, geopolitical and colonial), thus establishing a clear distinction between the expansionary, geopolitical and asymmetric ambitions of other actors.

---

[96] European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Establishing the European Defence Industrial Development Programme Aiming at Supporting the Competitiveness and Innovation Capacity of the Union's Defence Industry.*

[97] European Commission, *A New Industrial Strategy for Europe COM(2020) 102 Final*, Brussels, 2020, 1–16, https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf.

[98] European Commission.

[99] Interviewee A, interview by author, virtual (online video), March 5, 2021.

[100] Emphasis added, European Commission*, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's Digital Future.*

The distinctiveness—and autonomy—of Europe in cyberspace has been expressed by the Commission's 2020 Communication, *Shaping Europe's Digital Future,* which defined European technological sovereignty 'by focusing on the needs of Europeans and of the European social model.'[101] In this regard, the EU's assertion of 'sovereignty' is also reflective of the belief that the EU should retain its position as a 'neutral actor' in cyberspace.[102] Rather than acting 'passively' or as a 'tag along' to the US, sovereignty conveys that the EU is taking ownership of its own ambitions and security in a responsible way—to remain neutral, the EU must remain *independent* or *autonomous* from China and the US. Therefore, through the construction of 'European sovereignty' in official discourses, the EU has sought to differentiate itself from the invasive and *Westphalian* geopolitical aims of other cyber actors (particularly Russia and China) and from the competitive goals of the US.

A Strong Foundation?

In his 2018 *State of the Union Speech*, Juncker laid out the distinctively 'European' conception of sovereignty: that it was 'shared internally' and 'unified externally.'[103] However, the *internal* facet to this conception has yet to be realized. There remains internal contestation between EU policymakers and stakeholders surrounding the usage and meaning of sovereignty in EU policy discourse and thus deep instabilities underlying the concept. According to one policy expert, this contestation is a 'big Franco-German story' which has 'gotten more complicated' and 'less clear over time' (Interviewee C, 2021).[104] Whereas France advocated for the idea of European *strategic autonomy*, Germany advanced the argument for *European sovereignty*, as Germans believed that autonomy was 'too anti-American'.[105] Indeed, she

[101] European Commission, 2.
[102] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021.
[103] Juncker, "State of the Union 2018: The Hour of European Sovereignty."
[104] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[105] Interviewee C, interview by author.

contends, 'some in the US kind of made the same point' (Interviewee C, 2021).[106] However, complicating matters further, the French President Macron interpreted sovereignty in the 'reverse way' to the German conception; rather than encompassing the 'ability to act' (*handlungsfähigkeit*), he interpreted it as something unattainable for Europe—as 'oh, we're never going to reach sovereignty, sovereignty is a really big thing' (Interviewee C, 2021).[107] In comparison, he conceived of autonomy as a somewhat 'scaled down version' of sovereignty. However, the Germans were 'leading in this debate', which is what led to the emergence of the notion of sovereignty over autonomy. To date, the EU-level position about sovereignty is more reflective of the German conception of sovereignty (e.g. the capacity to act independently, as detailed in the previous section).

This conceptual *incoherence* is further indicated by survey data on 'European Sovereignty' conducted by Ipsos Public Affairs in late December 2020-Janurary 2021. This survey asked 8000 EU citizens of varying ages in France, Germany, Italy, Spain, Poland, Romania, Latvia, and Sweden (1000 per country) about the meaning of 'European sovereignty', particularly how it compared with 'national sovereignty', and whether it carried positive and negative connotations for respondents. This study found that opinions on the concept of European sovereignty were 'very mixed'. Whereas it was viewed positively by a majority of Germans, Poles, Romanians, Latvians, and Swedes, only a *minority* of French, Spanish, and Italian respondents viewed it positively (refer to Appendix 3.3 for further reference).[108]

Internal EU contestation regarding the usage of 'autonomy' versus 'sovereignty' has resulted in insecurities about conceptual misunderstandings with other external actors. This is particularly noticeable in interviewee responses, who raised concerns about the EU's

[106] Interviewee C, interview by author.
[107] Interviewee C, interview by author.
[108] Fondation Jean-Jaurès and Friedrich-Ebert-Stiftung, "Survey on European Sovereignty Carried out by Ipsos on Behalf of the Fondation Jean-Jaurès and the Friedrich-Ebert-Stiftung," 2020.

misperception as 'an island' and as shirking its strategic transatlantic ties.[109] As one official expressed, 'If you use the term sovereignty then it is like a red light on [us] because everybody's like sovereignty, this is [an] international organisation, what the heck, how are you going to interpret it?' (Interviewee A, 2021). [110] This anxiety encapsulates both French concerns about the use of 'sovereignty', and German concerns about the use of 'autonomy' as hurting transatlantic relations. Other interviewees at the EU Commission and the UK civil service respectively conveyed their exasperation about uncovering the meaning of these terms.[111]

Overall, the emergence of European sovereignty in EU policy discourses was a fractured process, and it remains a subject of internal debate for EU Member States. Member States' disagreement continues to stymie internal conceptual coherence about the meaning of European sovereignty. In the perspective of one policy expert, 'we are a bit stuck now' as a result of this internal contestation (Interviewee C, 2021).[112] The belief that Member States remain at an impasse regarding the application of *European* sovereignty is similarly corroborated by an interviewed Member State representative. They observed that there remains a divide in the Council regarding how Member States approach the meaning of *European* sovereignty—for about one half of the Council, European sovereignty includes openness, including with respect to the internal market, whereas the other side is more protectionist towards the internal market and EU borders (Interviewee B, 2021).[113] To this end, one official hoped that 'people will start to stop asking what this digital sovereignty means, but actually look at what we're doing on substance', as 'it's been a long road of trying to explain what it means and what it doesn't mean' (Interviewee E, 2021).[114]

[109] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021.

[110] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video).

[111] Interviewee E, interview by author, virtual (online video), March 25, 2021. Interviewee F, interview by author, virtual (online video), April 15, 2021.

[112] Interviewee C, interview by author, virtual (online video), March 12, 2021.

[113] Interviewee B, interview by author, virtual (online video), March 11, 2021.

[114] Interviewee E, interview by author, virtual (online video), March 25, 2021.

Brussels' decision to place the concept of 'digital sovereignty' at the forefront of the EU's new cybersecurity strategy, *Shaping Europe's Digital Future* (2020) in spite of this internal disagreement demonstrates the importance of the concept for the EU's ontological security and its geopolitical concerns in cyberspace. Exploring this concept has demonstrated that external appearances of unity and clarifying the EU's intentions in cyberspace are highly important, despite the presence of multiple competing views about sovereignty within Europe. It remains to be seen whether tensions between the internal and external facets to the concept will shatter the EU's self-construction as a cyber actor in the future.

Conclusion

This chapter has demonstrated how the EU's adoption of geopolitical and sovereigntist language was an interrelated process, shaped by, on the one hand, the further integration of cybersecurity policy with the EU's new global outlook (formalized by the EUGS), and on the other, ontological insecurities about geopolitics in cyberspace. It documents explicit examples of the EU 'speaking in geopolitical terms', which have included identifying other geopolitical actors as 'systemic rivals' and openly advocating for European sovereignty 'at this geopolitical hour'. However, as this exploration revealed, there are also more subtle traces of geopolitical thinking in EU cybersecurity policy. A key motivator for Member States' support of the 'sovereignty' concept was the realization that Member States could not 'act alone' in the current geopolitical context; for EU policymakers, the concept was seen as necessary to have 'conversations with the big geopolitical powers', including in 5G discussions. Accordingly, it also explored how geopolitics and sovereignty have emerged as ontologically intertwined concepts in the EU cybersecurity policy context.

Moreover, I have argued that 'European sovereignty' has been leveraged by policymakers as strategy to mitigate the EU's ontological insecurities about cyberspace—

particularly, its anxieties about how others perceive its identity, and its internal insecurities about how its identity should be constructed. However, internal disagreement between various constituent members of the EU collective have undermined the credibility and intelligibility of this 'European sovereignty' narrative. While it appears coherent with the EU's broader foreign policy aspirations to secure 'European sovereignty', enduring internal tensions and disagreement demonstrate that the concept has received mixed reception by the EU's partners and within the EU itself. As a consequence, the 'European digital sovereignty' hosts its own discursive instabilities which have detracted from its overall *meaning* to EU cybersecurity policy and the EU's self-representation as a cyber actor.

Chapter VII – Conclusion

'Whoever fights monsters should see to it that in the process he does not become a monster. And if you gaze long enough into an abyss, the abyss will gaze back into you.'
-Friedrich Nietzsche

Despite the myriad ways that our current world challenges the traditional foundations of geopolitics, geopolitical concepts have endured as key reference points for not only nation-states, but non-traditional state actors such as the European Union. This is demonstrated, for instance, with HR/VP Borrell's recent assertion that traditional geopolitics are renascent in cyberspace. His statement squeezes cyberspace into the Westphalian mould of international relations as occurring among 'bordered power containers.' Yet, paradoxically, the EU has continuously sought to elude this 'territorial trap' in constructing itself as a cyber actor.

This dissertation has explored how cyberspace—rather than fitting neatly within the trinitarian framework outlined above—has opened up a Pandora's box of insecurities for EU policymakers with which they have been grappling for nearly two decades. Specifically, my study traced the emergence of geopolitical and sovereigntist language in EU official discourses throughout the 2009-2020 time period. It principally argued that this development was the consequence of how EU policymakers have leveraged *distinctive* strategies—temporal, relational, and spatial othering—to mitigate the EU's ontological insecurities in cyberspace. These responses led to the legitimization of geopolitics in EU official discourses and the adoption of *European sovereignty* as a form of differentiation from other cyber actors. Overall, it demonstrated how the EU's self-orientation towards cyberspace has continued to come into tension with growing efforts to 'geopoliticize' cyberspace, both within and outside of the EU context.

Empirically, my study detailed how EU policymakers' responses to ontological insecurities through various strategies of 'othering' have changed in form over time and in

accordance with the loci of insecurity throughout the 2009-2020 period. It argued that this timeframe was characterized by three particular developments in EU cybersecurity policy discourse: the delegitimization of geopolitics (2009-2013), a period of rupture and reconceptualization of the EU's role in the global security environment (2014-mid 2017), and the legitimization of geopolitics and sovereigntist discourse (late 2017-2020). In the first phase of the EU's cyber policy development, the securitization of cyberspace and the EU's perceived autobiographical insecurities enabled the continued delegitimization of geopolitics in official EU discourses. In turn, the experience of multiple security crises in the EU's Neighbourhood and its interactions with other global actors instigated an existential crisis for the EU, which led to the reconceptualization of its role as a global actor. This reconceptualization deeply impacted the trajectory of EU cybersecurity policy, spurring the integration of new spatial and relational concepts into cyber policy discourse and the legitimization of geopolitical language. After experiencing further insecurities about how this shift would be perceived by other actors, policymakers began to adopt the discourse of 'European sovereignty' in order to differentiate the EU from geopolitical actors in cyberspace.

By focusing upon the particular ideational and political contexts in which geopolitical and sovereigntist concepts have been discussed in the case of the EU, this study has sought to move beyond the state-centric and materialist foci of extant scholarship on cyber geopolitics. In so doing, I was able to foreground how EU policymakers have negotiated the tensions between cyberspace and state-centric, realist assumptions to security, and to explore how the EU's ontological approach to cyberspace has evolved over time in response to important transformative events. Thus, this research produced two significant empirical findings. *First*, my analysis indicates that the EU's emergent geopolitical awareness and sovereignty concerns have been primarily oriented towards *state* cyber actors. As the 5G network dispute has revealed, EU officials' geopolitical concerns have largely concentrated upon *state-backed*

cyber activities, such as monitoring foreign direct investment to Chinese state-sponsored tech companies within the EU. This is further illustrated by policymakers' anxieties about weaponizing interdependencies in cyberspace, which have coalesced around powerful states actors (such as China and the US) as opposed to large companies such as Alphabet (Google) or Huawei. To a considerable extent, this state-centric focus appears to draw upon the realist or 'power-politics' conception of geopolitics, which focuses upon the seizure of territorial and material resources by powerful states.

Ontologically, this suggests that EU policymakers have drawn upon a Westphalian conception of geopolitics (which is characterized by a focus upon the sovereign nation-state) to approach the cyber environment. As argued in Chapter VI, policymakers have increasingly emphasized the importance of enhancing the EU's cyber capabilities and leveraging existing material instruments—such as the Euro—in order to further ensure the EU's sovereignty in cyberspace and to have 'credible conversations' with the 'big geopolitical players.' Indeed, as Borrell's most recent speech on cyber diplomacy revealed, the EEAS has asserted a determinedly 'geopolitical' 'power-politics perspective' to cyber issues to characterize its contemporary strategic approach to cyberspace.[1] In this Westphalian-oriented conception of the cyber environment, the main sources of insecurities are increasingly powerful state actors capable of weaponizing interdependencies for strategic goals or state-sponsored technology companies (although there are of course nuances to this threat perception).

Yet, my research has evidenced how—simultaneously—the EU has continued to represent itself as a *post-Westphalian* actor in cyberspace, through engaging in discursive strategies which construct (and reproduce) the EU's identity in opposition to a relational, geopolitical Other. Most recently, 'European sovereignty' was included to bolster this broader strategy of differentiation (as Chapter VI demonstrated). The EU has therefore continued to position itself

[1] Borrell, "Cyber Diplomacy and Shifting Geopolitical Landscapes," September 14, 2020.

as *transcendent* of the Westphalian and geopolitical context, while nonetheless engaging with power-politics concepts to make sense of other cyber actors and the strategic environment.

Considering these competing but interrelated dynamics, there appears to be a symbiotic relationship between geopolitical concepts and the EU's construction of its role as a cyber actor. The EU seems to be unable to escape the spectre of geopolitics—and moreover, it appears to be *unwilling* to do so—despite the structural opportunities cyberspace provides for the EU to move beyond geopolitics and the territorial trap more broadly. As documented in Chapters IV, V, and VI, EU policymakers are indeed aware of the subversive (or unique) features of cyberspace, evinced through officials' various concerns about (inter)dependency and the loss of control over technology and rules-setting in cyberspace due to its 'borderless' nature. These concerns, which encapsulate underlying anxieties about sovereignty and security, have been complicated by the dynamics of European integration and questions about a 'European-centric' approach (as discussed in Chapter IV).

Despite these tensions, EU policymakers have elevated the importance of geopolitics in cyberspace in the EU's strategic posture and advanced a narrative which draws upon a traditional principle of the European security order: sovereignty.[2] Geopolitics, then, remains an important source of material for the EU to reshape its identity and role as an actor. Cogent to this phenomenon is Merje Kuus' insight that, 'even claims about "escaping" geography and geopolitics are geopolitical insofar as they assume a particular geographical configuration of power that is to be eluded.'[3] Further research (particularly focusing upon the informal and internal dynamics which underlie this official narrative) would help to clarify the nuances in this ontological approach, and identify potential alternative representations of the EU or cyberspace not uncovered by this study.

[2] European Union, "Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy."

[3] Kuus, *Geopolitics Reframed : Security and Identity in Europe's Eastern Enlargement,* 7.

Secondly, this study can respond to the expectations of intergovernmentalist approaches about the EU's policy behaviour in cyberspace. Whereas intergovernmentalists would expect national sovereignty claims to 'leave the EU toothless', and thus unable to project the singular claim of 'European sovereignty' (e.g. Sliwinski's prediction),[4] this thesis has empirically demonstrated that national sovereignties have *not* precluded the development of the 'European sovereignty' concept (despite competing Member State conceptions of the term). Rather, debates at the Member State level have been centred upon solutions to addressing a *shared anxiety* about Europe's loss of sovereignty as a whole and concerns about how the EU could be misperceived as a geopolitical actor. Thus, internal contestation has been largely focused upon whether, and how, the concept of European sovereignty would be (mis)interpreted by *external* actors*,* as opposed to divided opinions between Member States about whether the concept interferes with their *own* sovereign claims. That is not to suggest intergovernmental dynamics do not matter—on the contrary, projections of European sovereignty at the EU level could reflect an internal logic of 'power multiplier' and (some) Member States' continued belief that of the value for a 'European-centric' approach to security. However, as this study revealed, Member States' motives are not the only drivers of this European sovereignty narrative—its emergence in discourses at the EU level (advanced by Juncker, Mogherini, and Barroso, as well as my interviewees) underscores the significant extent to which influential discussions about cybersecurity have been held above the national level. Indeed, my research has shown that traditional discussions about security have increasingly taken place within EU contexts—whereby Member States have come to view the EU as a 'welcome player' in geopolitical discussions.

Through exploring the specific case of EU cybersecurity policy, this dissertation was also able to consider more general normative and theoretical questions. For one, if ontological

[4] Sliwinski, "Moving beyond the European Union's Weakness as a Cyber-Security Agent," 470.

security entails what one wants to '*become'* as opposed to solely *'being'* (recalling Mitzen),[5] then what does this articulation of 'European sovereignty' mean for the EU's development as a political actor? The conceptual disagreements about 'European sovereignty' amongst EU Member States has raised the important question of whether *European sovereignty* entails '*EUropean* sovereignty' or state-based '*European* sovereignty'. Interviewee responses and textual analyses of this study are inconclusive—in fact, one interviewee raised this ambiguity as a significant issue in the EU policy context.[6] The fact that this ambiguity exists is worthy of further scrutiny; it suggests that Member State Representatives and EU officials have not established a clear distinction between the two versions of 'sovereignty'. Not unlike cyberspace, this dynamic reflects the EU's ambiguous entanglement with Westphalian and post-Westphalian concepts and exemplifies how the EU's external projections of a unified approach often belie internal contestation.

Recalling Pohle and Thiele's (2020) warning, the concept of digital sovereignty is 'not an end in itself,'[7] and as the epigraph for this chapter suggests, the EU's usage of geopolitical concepts and sovereignty language could have significant implications for its evolution as a political actor. The EU's engagement with geopolitics after its longstanding eschewal of the concept has opened up opportunities for further reconstructions of the EU's political identity, which could lead to a further embrace of 'traditional geopolitical thinking' in its external relations approach, as scholars have suggested in other policy areas.[8] It also opens the EU up to further critiques about its historical engagement with geography, as it can no longer deny that it 'has never thought that way' (Interviewee C, 2021).[9] After all, this study revealed that geography has remained 'at the centre of the [EU's] design'[10] as a political community, which

[5] Mitzen, "Anxious Community: EU as (in)Security Community," 398.
[6] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[7] Pohle and Thiel, "Digital Sovereignty," 14.
[8] Cadier, "The Geopoliticisation of the EU's Eastern Partnership"; Nitoiu and Sus, "Introduction: The Rise of Geopolitics in the EU's Approach in Its Eastern Neighbourhood."
[9] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[10] Nitoiu and Sus, "Introduction: The Rise of Geopolitics in the EU's Approach in Its Eastern Neighbourhood."

was demonstrated by the spatial logics embedded within its cyber capacity building programmes (analysed in Chapter V).

At the same time, as I have discussed above, the varied meaning of 'European sovereignty' for EU members suggests that it is still in the process of internal consolidation. While it projects a strong image, the 'European sovereignty' concept in EU cyber policy discourse emblematizes the inherent 'undecidability' of discursive constructions—that is, the possibility for agents to destabilize or overturn the concept's extant meaning. Arguably, the use of 'European sovereignty' to clarify and differentiate the EU's position in cyberspace is analogous to building a house out of glass: while it presents a polished front, it is a fragile construction that could shatter from internal pressure. It is too early to conclude whether 'European sovereignty' has precipitated a breakthrough in the EU's aspiration to become a 'forward-looking player in cyberspace' and a more coherent and empowered, global actor, or whether it has brought about its further destabilization. Potentially, the discursive transition from 'Member State sovereignties' to one 'European sovereignty' might precipitate a reshaping of the concept to be more inclusive of the EU's post-Westphalian identity as opposed to the intergovernmental sense of the term (e.g. 'pooled sovereignties'). Further research is required on the subject to understand the implications of this phenomena—and what this means for the EU's goals as a 'forward-looking cyber player'—in the digital era.

More broadly, the EU's engagement with 'sovereignty' in the context of cyberspace could present another opportunity for exploring the merits of the 'EU-as-empire' theory as advanced by Jan Zielonka and Kalypso Nicolaïdis, among others.[11] Focusing upon the ontological dimension of cyberspace facilitates the observation that cyberspace is analogous to an 'unsettled space' in the perspectives of traditional state or state-based actors. As this study has explored through its emphasis on *spatialization* and *externalisation*, actors have sought to

[11] Zielonka, *Europe as Empire: The Nature of the Enlarged European Union*; Nicolaïdis, Kalypso, Sebe, Berny, Maas, *Echoes of Empire: Identity, Memory and Colonial Legacies*; Fisher Onar and Nicolaïdis, "The Decentring Agenda: Europe as a Post-Colonial Power."

exert functional and territorial control over cyberspace through various attempts to 'settle it', by exporting their own models of governance, ideals/norms, and technologies. Thus, this analytical approach could serve as a point of departure for approaching cyberspace through a decolonial framework, which would not only serve as a refreshing alternative to the conventional state-centric and realist approaches, but it could help the discipline of IR break from its 'Westphalian mould' of analysis, as Kello called it. [12]

To summarize, this dissertation explored the implications of the emergence of geopolitics and sovereigntist language in contemporary EU cybersecurity policy discourse through the framework of *ontological insecurity*. An ontological insecurity lens revealed the significant extent to which conceptual assumptions influence policy discussions, including debates about how to approach cybersecurity (from a national, regional, or global level, for instance), and the EEAS' later realization that cyber threats required a fundamental shift from the EU's 'traditional mindset'. Additionally, exploring the development of EU cybersecurity policy over time reveals the significant extent to which existential anxieties may implicate problem-solving—such as adopting *external instruments* to address 'borderless' problems—or going to great lengths to avoid being misconstrued as a particular *type* of actor.

In conclusion, this dissertation aimed to establish the importance of not only investigating *whether* the EU can assert sovereign or geopolitical claims, but more fundamentally, to uncover *what has motivated* its pursuit of these concepts in the first place. Exploring the underlying ontological context reveals its influence upon policymakers' decision-making and makes it possible to conceive of why the EU has adopted geopolitical and sovereigntist language in its cybersecurity policy. An ontological insecurity framework also reveals that the EU has been grappling with a multitude of existential questions about its political identity as an actor—some of which remain unanswered. The EU's positioning in the

[12] Kello, *Virtual Weapon Int. Order*.

new ‘digital decade’ thus presents a rich area for further research on European integration in the more networked and digitalized context.

Bibliography

Adee, Sally. “The Global Internet Is Disintegrating. What Happens Next?” BBC, May 15, 2019. https://doi.org/10.1002/esp.1977.

Agnew, John. “The Territorial Trap: The Geographical Assumptions of International Relations.” *Review of International Political Economy* 1, no. 1 (1994): 53–80.

Aharon Klieman. *Great Powers and Geopolitics: International Affairs in a Rebalancing World*. Springer Press, 2015. http://www.springer.com/series/10201.

Akchurina, Viktoria, and Vincent Della Sala. “Europe and the Ontological Security Dilemma: Narrating the Emerging Eurasian Space.” *Europe-Asia Studies* 70, no. 10 (2018): 1638–55. https://doi.org/10.1080/09668136.2018.1546829.

Aleksandrowicz, Tomasz R. “Cyberspace as a Source of Threat to National Security. An Attempt to Conceptualize the Problem.” *Internal Security* 7, no. 1 (2015): 187–204. https://doi.org/10.5604/20805268.1192777.

American Journal of Managed Care. “A Timeline of COVID 19 Developments in 2020,” January 1, 2021. https://doi.org/10.1200/JCO.20.02608.

Bacchi, Carol Lee, and Susan Goodwin. *Poststructural Policy Analysis: A Guide to Practice*. Palgrave MacMillan, 2016.

Baezner, Marie. “Hotspot Analysis: Cyber and Information Warfare in the Ukrainian Conflict.” Zurich, 2018. www.css.ethz.ch.

Balzacq, Thierry. “The Three Faces of Securitization: Political Agency, Audience and Context.” *European Journal of International Relations* 11, no. 2 (2005): 171–201. https://doi.org/10.1177/1354066105052960.

Balzacq, Thierry, and Myriam Dunn Cavelty. “A Theory of Actor-Network for Cyber-Security.” *European Journal of International Security* 1, no. 2 (2016): 176–98. https://doi.org/10.1017/eis.2016.8.

Barbé, Esther, and Pol Morillas. “The EU Global Strategy: The Dynamics of a More Politicized and Politically Integrated Foreign Policy.” *Cambridge Review of International Affairs* 32, no. 6 (2019): 753–70. https://doi.org/10.1080/09557571.2019.1588227.

Barkawi, Tarak. “Decolonising War.” *European Journal of International Security* 1, no. 2 (2016): 199–214. https://doi.org/10.1017/eis.2016.7.

Barrinha, André. “Virtual Neighbors: Russia and the EU in Cyberspace.” *Insight Turkey* 20, no. 3 (2018): 29–41. https://doi.org/10.25253/99.2018203.02.

Barroso, Jose Manuel Durao. *European Commission 2004 – 2014: A Testimony by the President with Selected Documents*, 2014.

Bartolini, Stefano. *Restructuring Europe: Centre Formation, System Building, and Political Structuring between the Nation State and the European Union*. Online. Oxford: Oxford Scholarship Online, 2006. https://doi.org/10.1093/0199286434.001.0001.

Bendiek, Annegret, Minna Ålander, and Paul Bochtler. “CFSP: The Capability-Expectation Gap Revisited. A Data-Based Analysis,” 2020. https://www.swp-berlin.org/fileadmin/.

Bendiek, Annegret, Raphael Bossong, and Matthias Schulze. “The EU’s Revised Cybersecurity Strategy. Half-Hearted Progress on Far-Reaching Challenges,” 2017.

Bendiek, Annegret, Nadine Godehart, and David Schulze. “Global: The Age of Digital Geopolitics .” *International Politics and Society*, 2019. https://www.ips-journal.eu/regions/global/the-age-of-digital-geopolitics-3593/.

Bendiek, Annegret, and Eva Pander Maat. “The EU’s Regulatory Approach to Cybersecurity,” 2019.

Betz, David J., and Tim Stevens. “Analogical Reasoning and Cyber Security.” *Security*

Dialogue 44, no. 2 (2013): 147–64. https://doi.org/10.1177/0967010613478323.
Bevir, Mark, and Oliver Daddow. "Interpreting Foreign Policy: National, Comparative and Regional Studies." *International Relations* 29, no. 3 (2015): 273–87. https://doi.org/10.1177/0047117815600930.
Bialasiewicz, Luiza. *Europe in the World: EU Geopolitics and the Making of European Space* -. Edited by Luiza Bialasiewicz. Routledge, 2015. https://www.routledge.com/Europe-in-the-World-EU-Geopolitics-and-the-Making-of-European-Space/Bialasiewicz/p/book/9781138269347.
Blumenthal, Marjory S., and David D. Clark. "The Future of the Internet and Cyberpower." In *Cyberpower and National Security*, edited by F.D. Kramer, S. Starr, and L.K. Wentz. Washington: National Defense University Press, 2009.
Borg, Stefan. *European Integration and the Problem of the State*. 1st ed. London: Palgrave MacMillan, 2015. https://doi.org/10.1057/9781137409331.
Borrell, Josep. "Cyber Diplomacy and Shifting Geopolitical Landscapes," 2020.
———. "Cyber Diplomacy and Shifting Geopolitical Landscapes." European External Action Service, September 14, 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/85069/cyber-diplomacy-and-shifting.
Brizhinev, Dmitry, Nathan Ryan, and Roger Bradbury. "Modelling Hegemonic Power Transition in Cyberspace." *Complexity* 2018 (2018). https://doi.org/10.1155/2018/9306128.
Browning, Christopher S. "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War.'" *Political Geography* 62 (2018): 106–15. https://doi.org/10.1016/j.polgeo.2017.10.009.
Browning, Christopher S, and George Christou. "The Constitutive Power of Outsiders: The European Neighbourhood Policy and the Eastern Dimension." *Political Geography* 29 (2010): 109–18. https://doi.org/10.1016/j.polgeo.2010.02.009.
Browning, Christopher S, and Pertti Joenniemi. "Ontological Security, Self-Articulation and the Securitization of Identity." *Cooperation and Conflict* 52, no. 1 (2017): 31–47. https://doi.org/10.1177/0010836716653161.
Buzan, Barry, and Ole Wæver. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press, 2003.
Cadier, David. "The Geopoliticisation of the EU's Eastern Partnership." *Geopolitics* 24, no. 1 (2019): 71–99. https://doi.org/10.1080/14650045.2018.1477754.
———. "The Geopolitics of Eurasian Economic Integration." *LSE Ideas*, no. June (2014). http://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-Geopolitics-of-Eurasian-Economic-Intergration.pdf.
Cai, Cuhong. "Geopolitics in the Cyberspace: A New Perspective on U.S.-China Relations." *The Journal of International Studies* 39, no. 1 (2018). http://jtp.cnki.net/bilingual/detail/html/GJZY201801001?view=3.
Carbone, Maurizio. "The European Union and China's Rise in Africa: Competing Visions, External Coherence and Trilateral Cooperation." *Cooperation and Conflict* 29 (2011): 203–21. https://doi.org/10.1080/02589001.2011.555195.
Carrapico, Helena, and André Barrinha. "The EU as a Coherent (Cyber)Security Actor?" *Journal of Common Market Studies* 55, no. 6 (2017): 1254–72. https://doi.org/10.1111/jcms.12575.
Carrapico, Helena, and Benjamin Farrand. "Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy." *Journal of European Integration* 42, no. 8 (2020): 1111–26. https://doi.org/10.1080/07036337.2020.1853122.
Cash, John. "Psychoanalysis, Cultures of Anarchy, and Ontological Insecurity." *International Theory* 12, no. 306–321 (2020). https://doi.org/10.1017/S1752971920000147.

———. “To Dwell in Ambivalence: On the Promise and Dilemmas of Beck’s ‘the Art of Doubt’.” In *The Consequences of Global Disasters*, edited by A Elliot and E.L. Hsu, 169–181. New York: Routledge, 2016.

Choucri, Nazli, and David D. Clark. “Integrating Cyberspace and International Relations: The Co-Evolution Dilemma.” In *Explorations in Cyber-International Relations: Who Controls Cyberspace?* Cambridge: MIT Press, 2012.

Christou, George. *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*. Edited by Stuart Croft. *New Security Challenges Series*. Hampshire: Palgrave MacMillan, 2016. https://doi.org/10.1080/09662839.2016.1160892.

———. “The Collective Securitisation of Cyberspace in the European Union.” *West European Politics* 42, no. 2 (February 23, 2019): 278–301. https://doi.org/10.1080/01402382.2018.1510195.

———. “The EU’s Approach to Cyber-Security.” EU Commission Lifelong Learning Programme, 2017.

Ciot, Melania-Gabriela. “Cyberspace and the New World Order.” *Studia Universitatis Babeș-Bolyai Studia Europaea* 62, no. 2 (2014): 5–15.

Clarke, Adele E., Carrie Friese, and Rachel Washburn. *Situational Analysis in Practice: Mapping Research with Grounded Theory.* New York: Routledge: Taylor and Francis, 2015.

Cohen, Roger. “Bureaucracy Over Blood.” *New York Times*, February 24, 2007. https://archive.nytimes.com/www.nytimes.com/iht/2007/02/24/world/IHT-24globalist.html?pagewanted=print.

Council of Europe, European Union. “CyberEast.” Council of Europe, 2021. https://www.coe.int/en/web/cybercrime/cybereast.

Council of the EU Presidency. “Cyber Capacity Building: Towards a Strategic European Approach,” 2016.

Council of the European Union. *Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems.* Official Journal of the European Union L 69 (2005): 67–71.

———. *Proposal for a Directive 2013/27(COD) Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union 0027.* Brussels, 2013: 1–48. http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.

———. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: Establishing the European Defence Industrial Development Programme Aiming at Supporting the Competitiveness and Innovation Capacity of the Union’s Defence Industry*. SN 2717/18, no. Brussels, July 2018 (2018): 1–37.

Cruz Lobato, Luísa, and Kai Michael Kenkel. “Discourses of Cyberspace Securitization in Brazil and in the United States.” *Rev. Bras. Polít. Int* 58, no. 2 (2015): 23–43. https://doi.org/10.1590/0034-7329201500202.

Deibert, Ronald J., and Rafal Rohozinski. “Risking Security: Policies and Paradoxes of Cyberspace Security.” *International Political Sociology* 4, no. 1 (March 1, 2010): 15–32. https://doi.org/10.1111/j.1749-5687.2009.00088.x.

Demchak, Chris, and Peter Dombrowski. “Cyber Westphalia : Asserting State Prerogatives in Cyberspace.” *Georgetown Journal of International Affairs*, 2013, 29–38.

Diez, Thomas. “Europe’s Others and the Return of Geopolitics.” *Cambridge Review of International Affairs* 17, no. 2 (2004): 319–35. https://doi.org/10.1080/0955757042000245924.

———. “Normative Power as Hegemony.” *Cooperation and Conflict* 48, no. 2 (2013): 194–210. https://doi.org/10.1177/0010836713485387.

———. “Speaking ‘Europe’: The Politics of Integration Discourse.” *Journal of European*

Public Policy 6, no. 4 (1999): 598–613. https://doi.org/10.1080/135017699343496.
Dominioni, Samuele, and Fabio Rugge. “THE GEOPOLITICS OF 5G ,” September 2020. https://www.ispionline.it/sites/default/files/pubblicazioni/dossier_cyber_5g_september_2020.pdf.
Douzet, Frédérick. “Understanding Cyberspace with Geopolitics.” *Hérodote* 1, no. 152–153 (2014): 3–21. https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm.
Dunn Cavelty, Myriam. “European Politics and Society Europe’s Cyber-Power Europe’s Cyber-Power.” *European Politics and Society*, 2018. https://doi.org/10.1080/23745118.2018.1430718.
European External Action Service. *Food-for-Thought Paper: ‘Countering Hybrid Threats’*. Brussels, May (2015): 8. http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15. pdf.
Erlanger, Steven, and Katrin Bennhold. “For Europe, Cutting the Flow of Migrants Challenges Basic Ideals .” The New York Times, July 5, 2018. https://www.nytimes.com/2018/07/05/world/europe/migrants-merkel-kurz-austria.html.
EU Council. “Council Conclusions on Cyber Diplomacy” 2015, no. February (2015): 1–13. http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.
Eudaily, Seán Patrick, and Steve Smith. “Sovereign Geopolitics? Uncovering the ‘Sovereignty Paradox.’” *Geopolitics* 13, no. 2 (2008): 309–34. https://doi.org/10.1080/14650040801991621.
European Commission. Standard Eurobarometer: *EUROBAROMETER 74 AUTUMN 2010 INFORMATION ON EUROPEAN POLITICAL MATTERS REPORT*. Brussels, 2010. http://ec.europa.eu/public_opinion/index_en.htm.
European Commission. *5G Action Plan : Shaping Europe’s Digital Future*. Brussels, March 9, 2021. https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan.
———. *A Digital Agenda for Europe*. Brussels, 2010. ttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.
———. *A New Industrial Strategy for Europe. COM(2020) 102 Final*, Brussels, 2020. 1–16. https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf.
———. “Action Plan 5G for Europe2016 - Staff Working Document.” Brussels, 2016.
———*ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018. Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries*. Brussels, 2018.
———. *COMMISSION RECOMMENDATION of 26.3.2019 Cybersecurity of 5G Networks.* Brussels, 2019. https://doi.org/10.4018/978-1-7998-7708-0.ch029.
——— *COMMISSION RECOMMENDATION of 26.3.2019 Cybersecurity of 5G Networks.* Brussels, 2019. https://doi.org/10.4018/978-1-7998-7708-0.ch029.
———. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection. Brussels, 2009.
———. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe’s Digital Future*. Brussels, 2020.
———. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Twentieth Progress Report towards an Effective and Genuine Security Union. *Official Journal of*

the European Union. Brussels, 2019.
———. *Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Proposal for a Regulation of the European Parliament and of the Council*. *COM(2018) 630 Final*. Brussels, (2018).
———. "Eurobarometer Survey on Internal Security : The Economic Crisis and Terrorism Top the Agenda." *Memo*, no. November (2011).
———. *REFLECTION PAPER ON THE FUTURE OF EUROPEAN DEFENCE.* Brussels, 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0315.
———. "Secure 5G Networks : Questions and Answers on the EU Toolbox," no. January (2020). https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.
European Commission (SWD). "Staff Working Document: 5G for Europe: An Action Plan 2016 Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions Brussels," 2016. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=17131.
European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL EU-China – A Strategic Outlook*. Brussels, 2019.
———. *Joint Framework on Countering Hybrid Threats: A European Union Response.* Brussels, 2016.
European Commission, and High Representative of the Union for Foreign Affairs and Security Policy. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013. https://doi.org/10.4271/2010-01-1021.
———. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. JOIN(2017) 450 Fina*l. Brussels, 2017.
———. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Brussels, 2020.* https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.
European Commisssion. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection 'Achievements and next Steps: Towards Global Cyber-Securrity.* Brussels, 2011. http://publications.lib.chalmers.se/records/fulltext/245180/245180.pdf%0Ahttps://hdl.handle.net/20.500.12380/245180%0Ahttp://dx.doi.org/10.1016/j.jsames.2011.03.003%0Ahttps://doi.org/10.1016/j.gr.2017.08.001%0Ahttp://dx.doi.org/10.1016/j.precamres.2014.12.
———. *The European Agenda on Security*. Brussels, 2015. 1–21. https://doi.org/10.4324/9780429465918-2.
European Court of Auditors. "Audit Preview: Implementing Secure 5G Networks in the EU and Its Member States," 2020.
———. "The EU's Response to China's State-Driven Investment Strategy," no. 0 (2020).
European Institute for Security Studies. "Capacity Building in Cyberspace: Taking Stock (Event Report)." Brussels, November 19, 2013.
European Organization for Security. "Towards a Concerted EU Approach to Cyber Security," 2010. http://www.eos-eu.com/Files/Cuber-policy-docs/EOS_ICTWG_CyberSec_v5%200.pdf.

European Parliament. *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,* Pub. L. No. L 194/1, Official Journal of the European Union 58 (2016). https://doi.org/10.2307/j.ctt1xhr7hq.20.

———. *European Parliament resolution of 24 May 2007 on Estonia (2007).* https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0215+0+DOC+XML+V0//EN.

———. S*ecurity Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them*. Strasbourg, 2019.

European Union. *Association Agreement between the European Union and Its Member States, of the One Part, and Ukraine, of the Other Part*. Official Journal of the European Unio*n* L–161, no. 2014-02–29 (2014): 1–2137. https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf.

European Union. *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy.* Brussels, 2016, 1–56. http://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf.

European Union Agency for Cybersecurity (ENISA). "Cybersecurity Institutional Map," 2020. https://www.enisa.europa.eu/cybersecurity-institutional-map/results.

European Union Committee. "Protecting Europe against Large-Scale Cyber-Attacks." *House of Lords Publications*. London, 2010.

Fahey, Elaine. "The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security." Amsterdam, 2014.

Farrell, Henry, and Abraham L. Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1 (2019): 42–79. https://doi.org/10.1162/ISEC_a_00351.

Fearon, James D. "Cooperation, Conflict, and the Costs of Anarchy." *International Organization* 72, no. 3 (2018): 523–59. https://doi.org/10.1017/S0020818318000309.

Fisher Onar, Nora, and Kalypso Nicolaïdis. "The Decentring Agenda: Europe as a Post-Colonial Power." *Cooperation and Conflict* 48, no. 2 (2013): 283–303. https://doi.org/10.1177/0010836713485384.

Flockhart, Trine. "'Me Tarzan – You Jane': The EU and NATO and the Reversal of Roles." *Perspectives on European Politics and Society* 12, no. 3 (2011): 263–82. https://doi.org/10.1080/15705854.2011.596306.

———. "The Problem of Change in Constructivist Theory: Ontological Security Seeking and Agent Motivation." *Review of International Studies* 42, no. 5 (2016): 799–820. https://doi.org/10.1017/S026021051600019X.

Floridi, Luciano. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy and Technology* 33, no. 3 (2020): 369–78. https://doi.org/10.1007/s13347-020-00423-6.

Fondation Jean-Jaurès, and Friedrich-Ebert-Stiftung. "Survey on European Sovereignty Carried out by Ipsos on Behalf of the Fondation Jean-Jaurès and the Friedrich-Ebert-Stiftung," 2020.

Fossum, John Erik. "Conceptualizing the European Union Through Four Strategies of Comparison." *Comparative European Politics* 4 (2006): 94–123. https://doi.org/10.1057/palgrave.cep.6110077.

Gartzke, Erik, and Jon R Lindsay. "Security Studies Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," 2015. https://doi.org/10.1080/09636412.2015.1038188.

General Secretariat of the Council. *Council Conclusions: Mainstreaming Digital Solutions*

and Technologies in EU Development Policy. Brussels, 2016.

———.*EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018).* Brussels, 2018.

———. *Shaping Europe's Digital Future - Council Conclusions*. Brussels, June 9, 2020.

Giddens, Anthony. *The Nation State and Violence: Volume Two of A Contemporary Critique of Historical Materialism*. Cambridge: Polity, 1985.

Gravier, Magali. "Empire vs Federation: Which Path for Europe?" *Journal of Political Power* 4, no. 3 (2011): 413–31. https://doi.org/10.1080/2158379X.2011.628854.

Guitton, Clement. "Cyber Insecurity as a National Threat: Overreaction from Germany, France and the UK?" *European Security* 22, no. 1 (2013): 21–35. https://doi.org/10.1080/09662839.2012.749864.

Guzzini, Stefano. *The Return of Geopolitics in Europe?: Social Mechanisms and Foreign Policy Identity Crises*. Cambridge: Cambridge University Press, 2012. https://doi.org/doi:10.1017/CBO9781139225809.

Habermas, Jurgen. "The European Nation State. Its Achievements and Its Limitations. On the Past and Future of Sovereignty and Citizenship." *Ratio Juris* 9 (1996). https://heinonline.org/HOL/Page?handle=hein.journals/raju9&id=125&div=12&collection=journals.

Hansen, Lene. *Security as Practice: Discourse Analysis and the Bosnian War*. London: Routledge, 2006.

Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (2009): 1155–75. https://academic.oup.com/isq/article/53/4/1155/1815351.

Hay, Colin. "Political Ontology." In *The Oxford Handbook of Political Science*, edited by Robert E. Goodin. Oxford University Press, 2011. https://doi.org/10.1093/oxfordhb/9780199604456.013.0023.

Hix, Simon. "The Study of the European Community: The Challenge to Comparative Politics." *West European Politics,* 17, no. 1 (1994): 1–30. https://doi.org/10.1080/01402389408424999.

Hoffmann, Stanley. "Obstinate or Obsolete ? The Fate of the Nation-State and the Case of Western Europe." *Daedalus* 95, no. 3 (1996): 862–915.

Howorth, Jolyon, and Anand Menon. "Still Not Pushing Back: Why the European Union Is Not Balancing the United States." *Source: The Journal of Conflict Resolution* 53, no. 5 (2009): 727–44. https://doi.org/10.1177/0022002709339362.

Joenniemi, Pertti. "Re-negotiating Europe's Identity: The European Neighbourhood Policy as a Form of Differentiation." *Journal of Borderlands Studies* 23, no. 3 (2008): 83–94. https://doi.org/10.1080/08865655.2008.9695710.

Johansson-Nogués, Elisabeth. "The EU's Ontological (in) Security: Stabilising the ENP Area … and the EU-Self?" *Cooperation and Conflict* 53, no. 4 (2018): 528–44. https://doi.org/10.1177/0010836717750197.

Joque, Justin, and Taiabul Haque. "Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity; Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity," 2020. https://doi.org/10.1145/3442167.3442170.

Juncker, Jean-Claude. "State of the Union 2018: The Hour of European Sovereignty." European Commission, 2018. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en_0.pdf.

Juncos, Ana E. "Resilience as the New EU Foreign Policy Paradigm: A Pragmatist Turn?" *European Security* 26, no. 1 (January 2, 2017): 1–18. https://doi.org/10.1080/09662839.2016.1247809.

Kadercan, Burak. “Triangulating Territory: A Case for Pragmatic Interaction between Political Science, Political Geography, and Critical IR.” *International Theory* 7, no. 1 (2015): 125–61. https://doi.org/10.1017/S1752971914000402.

Karamanidou, Lena. “The Securitisation of European Migration Policies: Perceptions of Threat and Management of Risk.” In *The Securitisation of Migration in the EU*. Palgrave Macmillan UK, 2015. https://doi.org/10.1057/9781137480583.

Karyotis, Georgios. “European Migration Policy in the Aftermath of September 11. The Security-Migration Nexus.” *Innovation: The European Journal of Social Science Research* 20, no. 1 (2007): 1–17. https://doi.org/10.1080/13511610701197783.

Kello, Lucas. “Technological Revolution and International Order.” *The Virtual Weapon and International Order*, 2017, 80–116. https://doi.org/10.2307/j.ctt1trkjd1.8.

———. “The Quest for Cyber Theory.” In *The Virtual Weapon and International Order*, 23–57. Yale University Press, 2017. https://doi.org/10.2307/j.ctt1trkjd1.6.

———. *The Virtual Weapon and International Order*. Yale University Press, 2017. https://doi.org/https://doi.org/10.2307/j.ctt1trkjd1.

Kinnvall, Catarina. “Globalization and Religious Nationalism: Self, Identity, and the Search for Ontological Security.” *Political Psychology* 25, no. 5 (2004).

Kinnvall, Catarina, and Jennifer Mitzen. “Anxiety, Fear, and Ontological Security in World Politics: Thinking with and beyond Giddens.” *International Theory* 12 (2020): 240–56. https://doi.org/10.1017/S175297192000010X.

Krasner, Stephen D. “Compromising Westphalia.” Vol. 20, 1995. https://about.jstor.org/terms.

Kremer, Jan-Frederik, and Benedikt Müller. *Cyberspace and International Relations: Theory, Prospects and Challenges*. New York: Springer Press, 2014. https://www.springer.com/gp/book/9783642374807.

Król, Łukasz Antoni. “Digital Foreign Policy: How Digital Tools Can Further Europe’s Foreign Policy Goals.” *European View* 15, no. 1 (2016): 133–44. https://doi.org/10.1007/s12290-016-0384-8.

Kuehl, D. “From Cyberspace to Cyberpower: Defining the Problem.” In *Cyberpower and National Security*, edited by F. D. Kramer, S. H. Starr, and L.K. Wentz. Washington, DC: National Defense University Press, 2009.

Kuus, Merje. *Geopolitics Reframed : Security and Identity in Europe’s Eastern Enlargement*. Ebook: Palgrave Macmillan US, 2007.

———. “Policy and Geopolitics: Bounding Europe in EUrope.” *Annals of the Association of American Geographers* 101, no. 5 (2011): 1140–55. https://doi.org/10.1080/00045608.2011.577362.

Laclau, Ernesto, and Chantal Mouffe. *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso, 1985.

Laine, Jussi. “The Ukraine Crisis and Ontological (In)Security: Implications from a Finnish Perspective.” In *Ukraine after Maidan - Revisiting Domestic and Regional Security - Soviet and Post-Soviet Politics and Society*, edited by Tomasz Stępniewski and George Soroka, 212. Stuttgart: Ibidem-Verlag, 2018.

Lawson, Sean. “Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats.” *Journal of Information Technology and Politics* 10, no. 1 (January 2013): 86–103. https://doi.org/10.1080/19331681.2012.759059.

Lewis, James A. “Sovereignty and the Evolution of Internet Ideology,” 2020. https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology.

Leyen, Ursula Von der. “Political Guidelines for the next European Commission, 2019-2024,” 2020. https://doi.org/10.5771/2193-5505-2020-3-253.

Libicki, Martin C. *Conquest in Cyberspace*. Cambridge: Cambridge University Press, 2007.

Liebetrau, Tobias, and Kristoffer Kjærgaard Christensen. “The Ontological Politics of Cyber Security: Emerging Agencies, Actors, Sites and Spaces.” *European Journal of International Security*, 2020, 1–19. https://doi.org/10.1017/eis.2020.10.

Lindsay, Jon, Erik Gartzke, In Kelly, M Greenhill, and Peter J P Krause. “Coercion through Cyberspace: The Stability-Instability Paradox Revisited,” 2016.

Lucarelli, Sonia, and Lorenzo Fioramonti. *External Perceptions of the European Union as a Global Actor*. *External Perceptions of the European Union as a Global Actor*. Routledge Taylor & Francis Group, 2009. https://doi.org/10.4324/9780203866917.

Lutz, Philipp, and Felix Karstens. “External Borders and Internal Freedoms: How the Refugee Crisis Shaped the Bordering Preferences of European Citizens.” *Journal of European Public Policy*, February 11, 2021, 1–19. https://doi.org/10.1080/13501763.2021.1882541.

Maizland, Lindsay, and Andrew Chatzky. “Huawei: China’s Controversial Tech Giant .” Council on Foreign Relations, August 6, 2020. https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant.

Major, Claudia, and Christian Mölling. “A Hybrid Security Policy for Europe. Resilience, Deterrence, and Defense as Leitmotifs,” 2015.

Mälksoo, Maria. “Contemporary Security Policy From the ESS to the EU Global Strategy: External Policy, Internal Purpose,” 2016. https://doi.org/10.1080/13523260.2016.1238245.

———. “Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO.” *European Security* 27, no. 3 (2018): 374–92. https://doi.org/10.1080/09662839.2018.1497984.

Manners, Ian. “Normative Power Europe: A Contradiction in Terms?” *Journal of Common Market Studies* 40, no. 2 (June 1, 2002): 235–58. https://doi.org/10.1111/1468-5965.00353.

Maurer, Tim. “Cyber Proxies and the Crisis in Ukraine.” In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers. NATO CCD COE Publications, 2015. http://www.kyivpost.com/content/kyiv-.

Mitzen, Jennifer. “Anxious Community: EU as (in)Security Community.” *European Security* 27, no. 3 (2018): 393–413. https://doi.org/10.1080/09662839.2018.1497985.

———. “Feeling at Home in Europe: Migration, Ontological Security, and the Political Psychology of EU Bordering.” *Political Psychology* 39, no. 6 (2018). https://doi.org/10.1111/pops.12553.

Mogherini, Federica. “Speech by HR/VP Mogherini at the EUISS Annual Conference, Towards an EU Global Strategy-The Final Stage ,” April 22, 2016.

Morgenthau, Hans J. *Politics Among Nations : The Struggle for Power and Peace*. 4th ed. New York NY: Alfred A. Knopf, 1948.

NATO Cooperative Cyber Defence Centre of Excellence. “2007 Cyber Attacks on Estonia,” 2007.

Nicolaïdis, Kalypso, Sebe, Berny, Maas, Gabrielle. *Echoes of Empire: Identity, Memory and Colonial Legacies*, 2015. www.ibtauris.com.

Niemann, Arne, Charlotte Bretherton, and Johannes Gutenberg. “EU External Policy at the Crossroads: The Challenge of Actorness and Effectiveness.” *International Relations* 27, no. 3 (2013): 261–75. https://doi.org/10.1177/0047117813497306.

NIS Cooperation Group. “EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks.” *European Commission*, 2019. https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

Nissenbaum, Helen. “Where Computer Security Meets National Security .” *Ethics and*

Information Technology 7 (2005): 61–73. https://doi.org/10.1007/s10676-005-4582-3.
Nitoiu, Cristian, and Monika Sus. “Introduction: The Rise of Geopolitics in the EU’s Approach in Its Eastern Neighbourhood.” *Geopolitics* 24, no. 1 (2019): 1–19. https://doi.org/10.1080/14650045.2019.1544396.
Noort, Carolijn Van, and Thomas Colley. “How Do Strategic Narratives Shape Policy Adoption? Responses to China’s Belt and Road Initiative.” *Review of International Studies* 47, no. 1 (2021): 39–63. https://doi.org/10.1017/S0260210520000388.
Nye, Joseph S. “The Regime Complex for Managing Global Cyber Activities.” *CIGI Publications*, no. 1 (2014): 1–15.
Nye Jr, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (2017): 44–71. https://doi.org/10.1162/ISEC_a_00266.
Ördén, H. “Deferring Substance: EU Policy and the Information Threat.” *Intelligence and National Security* 34, no. 3 (2019): 421–37. https://doi.org/10.1080/02684527.2019.1553706.
Ördén, Hedvig. “Deferring Substance: EU Policy and the Information Threat.” *Intelligence and National Security* 34, no. 3 (2019): 421–37. https://doi.org/10.1080/02684527.2019.1553706.
Pawlak, Patryk., Instrument contributing to Stability and Peace. European Commission, Unit "Security European Commission’s Directorate-General for International Cooperation and Development, EUISS Task Force for Cyber Capacity Building., and France) Institute for Security Studies (Paris. *Operational Guidance for the EU’s International Cooperation on Cyber Capacity Building*, 2018. https://doi.org/10.2815/38445.
Pawlak, Patryk. “Building Capacities for Cyber Defence.” *EUISS*, November 2017. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert 26 Cyber development.pdf.
———. “Cyber Capacity Building in Ten Points,” March 14, 2014.
———. “Understanding Hybrid Threats,” 2015. https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.
Pohle, Julia, and Thorsten Thiel. “Digital Sovereignty.” *Internet Policy Review* 9, no. 4 (2020): 1–19. https://doi.org/10.14763/2020.4.1532.
Politico-Military Group. “Six Monthly Report on the Implementation of the Cyber Defence Policy Framework.” Vol. 2016, 2016.
Pomorska, Karolina, and Sophie Vanhoonacker. “Europe as a Global Actor: Searching for a New Strategic Approach.” *Journal of Common Market Studies* 54, no. April (2016): 204–17. https://doi.org/10.1111/jcms.12430.
Pop, Adrian. “From Cooperation to Confrontation: The Impact of Bilateral Perceptions and Interactions on the EU-Russia Relations in the Context of Shared Neighbourhood.” *Eastern Journal of European Studies* 7, no. 2 (2016): 47–70.
Powell, Matthew T. “Bestial Representations of Otherness: Kafka’s Animal Stories.” *Journal of Modern Literature* 32, no. 1 (2008): 129–42. https://www.jstor.org/stable/25511795?seq=1#metadata_info_tab_contents.
Powers, Shawn M., and Michael Joblanski. *The Real Cyber War : The Political Economy of Internet Freedom*, 2015. https://ebookcentral.proquest.com/lib/oxford/detail.action?docID=3414433.
Renard, Thomas. “EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain.” *European Politics and Society* 19, no. 3 (2018): 321–37. https://doi.org/10.1080/23745118.2018.1430720.
Rid, Thomas. “Cyber War Will Not Take Place.” *Journal of Strategic Studies* 35, no. 1 (2012): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Rogers, James. “From ‘civilian Power’ to ‘Global Power’: Explicating the European Union’s ‘grand Strategy’ through the Articulation of Discourse Theory.” *Journal of Common Market Studies* 47, no. 4 (2009): 831–62. https://doi.org/10.1111/j.1468-5965.2009.02007.x.

Rovner, Joshua, and Tyler Moore. “Does the Internet Need a Hegemon?” *Journal of Global Security Studies* 2, no. 3 (July 1, 2017): 184–203. https://doi.org/10.1093/jogss/ogx008.

Rumelili, Bahar. “Integrating Anxiety into International Relations Theory: Hobbes, Existentialism, and Ontological Security.” *International Theory* 12 (2020): 257–72. https://doi.org/10.1017/S1752971920000093.

Sălăjan, Loretta. “Ontological Security and the European Union Global Strategy.” *Revista de Stiinte Politice*, no. 58 (2018): 23–33.

Schwartz-Shea, Peregrine, and Dvora Yanow. *Interpretive Design: Concepts and Processes.* New York NY: Routledge, Taylor & Francis, 2012.

Secretary General/High Representative. A Secure Europe in a Better World: European Security Strategy, Pub. L. No. PESC 787 (2003). https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf.

Segal, Adam. “Huawei, 5G and Weaponized Interdependence.” In *The Uses and Abuses of Weaponized Interdependence*, edited by Daniel W. Drezner, Henry Farrell, and Abraham L. Newman. Brookings Institution Press, 2021.

Sjursen, Helene. “Not so Intergovernmental after All? On Democracy and Integration in European Foreign and Security Policy.” *Journal of European Public Policy* 18, no. 8 (2011): 1078–95. https://doi.org/10.1080/13501763.2011.615194.

Sliwinski, Krzysztof Feliks. “Moving beyond the European Union’s Weakness as a Cyber-Security Agent.” *Contemporary Security Policy* 35, no. 3 (2014): 468–86. https://doi.org/10.1080/13523260.2014.959261.

Special Eurobarometer. “Special Eurobarometer 404 Cyber Security,” 2013. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf.

Starr, Stuart H. “Toward a Preliminary Theory of Cyberpower.” In *Cyberpower and National Security*, 2009.

Stevens, Tim. *Cyber Security and the Politics of Time*. *Cyber Security and the Politics of Time*. Cambridge: : Cambridge University Press, 2016. https://doi.org/10.1017/CBO9781316271636.

Subotic, Jelena. “Narrative, Ontological Security, and Foreign Policy Change .” *Foreign Policy Analysis* 12, no. 6 (2016). https://doi.org/10.1111/fpa.12089.

Taddeo, Mariarosaria. “Cyber Conflicts and Political Power in Information Societies.” *Minds and Machines* 27, no. 2 (2017): 265–68. https://doi.org/10.1007/s11023-017-9436-3.

Tarantino, Luca. “The 5G Moment of Truth in Europe: Geopolitical Implications, Economic Opportunities and Cybersecurity Concerns,” 2020.

The New York Times. “The Tech Cold War Between the U.S. and China Is Heating Up,” 2020. https://www.nytimes.com/2020/10/01/business/dealbook/tech-cold-war-us-china.html.

Torfing, Jacob. *New Theories of Discourse: Laclau, Mouffe and Žižek*. Oxford: Blackwell Publishing Ltd, 1999.

Traynor, Ian. “Russia Accused of Unleashing Cyberwar to Disable Estonia .” The Guardian, May 17, 2007. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

Trimintzios, Panagiotis, Georgios Chatzichristos, Silvia Portesi, Prokopios Drogkaris, Lauri Palkmets, Dimitra Liveri, and Andrea Dufkova. “Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU.” Brussels, 2017.

Vollaard, Hans. *European Disintegration : A Search for Explanations*. Palgrave S. New York: Palgrave MacMillan, 2018.

Walt, Stephen M. “The Renaissance of Security Studies.” *International Studies Quarterly,* 35, no. 2 (1991): 211. https://doi.org/10.2307/2600471.

Weber, Valentin. “Making Sense of Technological Spheres of Influence.” London, 2020. https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Technological-Spheres-of-Influence.pdf.

Weiler, Joseph. “Europe Must Learn Quickly to Speak the Language of Power.” *EJIL: Talk! Blog of the European Journal of International Law*, October 29, 2020. https://www.ejiltalk.org/europe-must-learn-quickly-to-speak-the-language-of-power-part-i/.

Wong, Reuben, and Christopher Hill. “National and European Foreign Policies: Towards Europeanization.” *National and European Foreign Policies: Towards Europeanization*, no. April (2012): 1–280. https://doi.org/10.4324/9780203816035.

Zanders, Jean-Pascal. “Cyber Security: What Role for CFSP?” *European Union Institute for Security Studies*. Brussels, 2009.

Zanon, Bruno. “Infrastructure Network Development, Re-Territorialization Processes and Multilevel Territorial Governance: A Case Study in Northern Italy.” *Planning Practice and Research* 26, no. 3 (2011). https://doi.org/10.1080/02697459.2011.580114.

Zekos, Georgios I. “Demolishing State’s Sole Power over Sovereignty and Territory Via Electronic Technology and Cyberspace.” *Journal of Internet Law* 17, no. 5 (2013): 3–17. http://proxy.lib.sfu.ca/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=91743838&site=ehost-live.

Zielonka, Jan. “Europe’s New Civilizing Missions: The EU’s Normative Power Discourse.” *Journal of Political Ideologies* 18, no. 1 (February 2013): 35–55. https://doi.org/10.1080/13569317.2013.750172.

———. *Europe as Empire: The Nature of the Enlarged European Union*. Vol. 9780199292. Oxford University Press (OUP), 2006. https://doi.org/10.1093/0199292213.001.0001.

Appendices

Appendix 1 – Literature Review (Chapter 2)

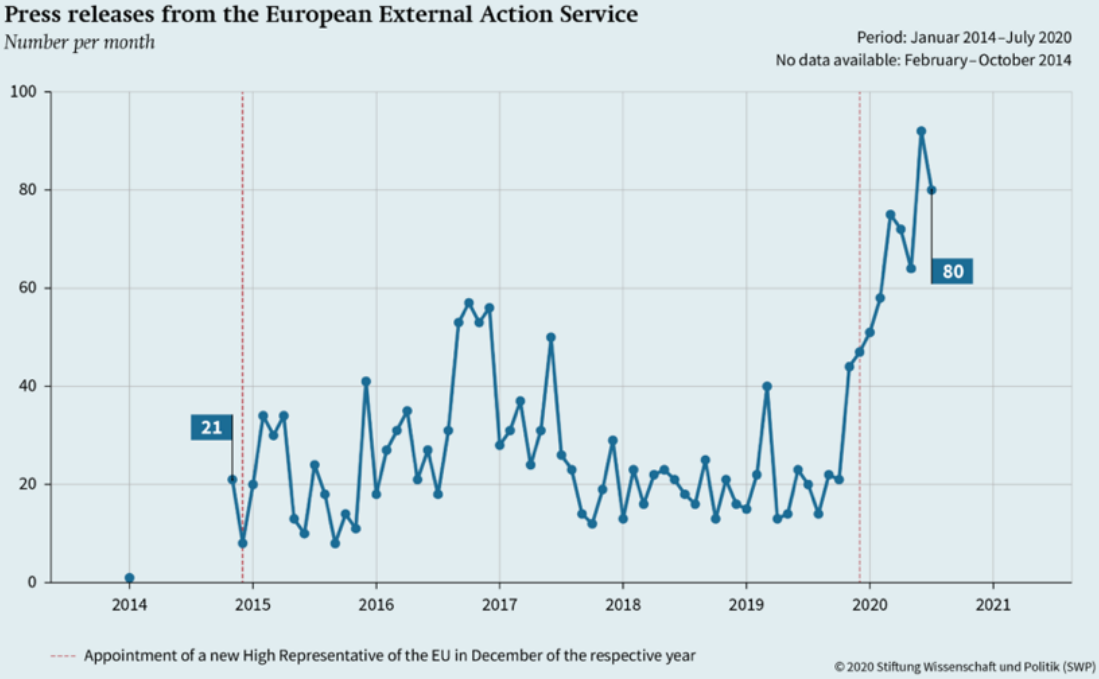
Appendix 1.

Number of press releases from the External Action Service (often released in the absence of an EU Council policy decision) over the January 2014-July 2020 time period, compiled by Ålander, Bendiek and Bochtler (2020).[1]

Chart 3

Press releases from the European External Action Service

Number per month



Source: Minna Ålander, Annegret Bendiek and Paul Bochtler, *A Critical Perspective on Data Transparency in the Common Foreign and Security Policy of the European Union*, Berlin: SWP Research Division EU / Europe, Working Paper (WP) 2020/no. 02, November 2020, https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP2020_Alander_et_al_Data-analysis_CFSP-output.pdf.

[1] Bendiek, Ålander, and Bochtler, "CFSP: The Capability-Expectation Gap Revisited. A Data-Based Analysis." (Open access document.)

Appendix 2 – Methodology (Chapter 3)

Appendix 2.1. - Inexhaustive List of EU Cyber Policy Communities (compilation is my own).

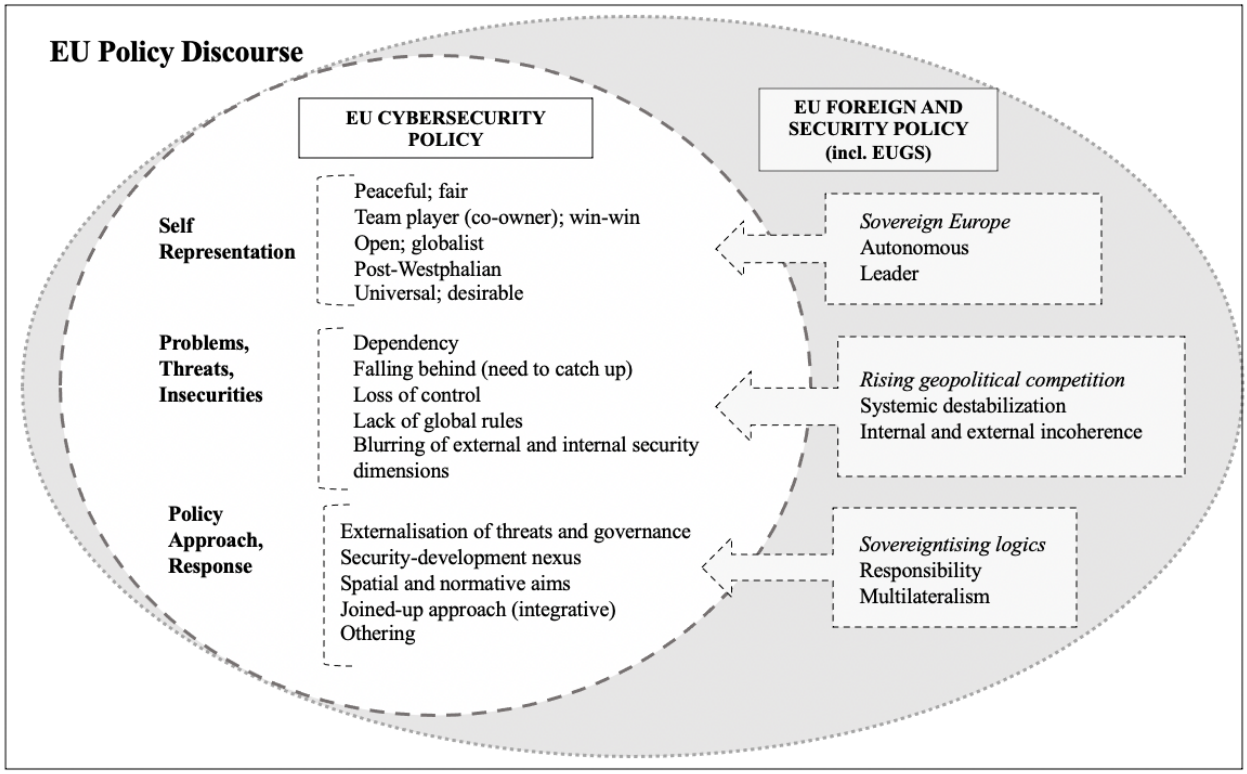
Inexhaustive List of EU Policy Communities (*compilation is my own*).	
Purpose	**Institutions/Organizations**
Creation of the CFSP/CDSP	- EU Council (Member State representatives, EU President, High Representative/Vice President of the European Commission – HR/VP) - Council of Ministers (national ministers) - External Action Service (EEAS: led by the HRVP, includes 'Eurodiplomats' and national delegates, est. 2010)
Associated or in collaboration with the CFSP/CDSP process	- Foreign Affairs Council (foreign ministers, members of the PSC) - Political and Security Committee of the European Parliament (PSC) - European Defence Agency* - Europol*/European Cybercrime Centre (EC3) - EU Institute for Security Studies (EUISS)
Cyber policymaking (including internal/domestic areas)	- European Agency for Cybersecurity (ENISA)* - Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU)
Associated with cyber policymaking	- Joint Research Centre (JRC: part of the European Commission) - The European Cybersecurity Organization (ECSO, est. 2016) - European Council on Foreign Relations
Influential organizations on cyber policy (in which EU Member States are participants)	- Council of Europe - UN - NATO** - OECD** - OSCE
Denotes a signatory of the* Memorandum of Understanding *(2019): quadrilateral cooperation with ENISA, Europol, CERT-EU, and the EDA, with the aim of improving cybersecurity and supporting Member States' defence programmes* * Denotes partial membership, with a majority of EU Member States as organizational members*	

Appendix 2.2. - Sample of emergent ideas relevant to ontological security, extracted during interpretive analysis.

Emergent Ideas relevant to Ontological Insecurity	Potential Insecurity Type (Context-dependent)
Loss of control over previously controllable entities or actors	Environmental; autobiographical
Lack of predictability in environment; acute disorientation or conceptual disagreement	Environmental
(Inter)dependency on uncontrollable actors or entities	Relational; environmental
Loss of trust or lack of trust (in other peers; or in the internal collective—e.g. Member States' Euroskepticism)	Autobiographical; relational
Declining self-esteem; and rising concerns about reputational costs	Autobiographical
Inability to 'keep up' with the pace of threats; *chronic* lack of preparedness	Autobiographical
Explicit references to 'existential crises', 'threats to fundamental existence/security'	Any

Appendix 3 –Legitimization and European Sovereignty (Chapter 6)

Appendix 3.1 – Visualization of Ideational Convergence between EU Cybersecurity and Foreign and Security Policy Discourses (EUGS), 2016-2020.



Appendix 3.2 - Relational Othering in EU Cyber Policy Discourse: Further Examples

In a broader sense, one interviewee contrasted the 'European approach' to geographical expansion and global engagement as different from a geopolitical enterprise. She discursively linked European enlargement to the EU's 'team-player' and 'open' disposition, commenting that 'for the Europeans […it is more about] sharing the cool things with others; bringing enlightenment to the rest of the world'. In the same breath, she differentiated this approach from the West's tendency to think about geopolitics and form alliances on such a basis (Interviewee C, 2021).[2] Elsewhere, the emphasis on openness and global, multilateral engagement is juxtaposed with protectionism and isolationism in the EUGS. Specifically, it asserts that, 'The Union cannot pull up a drawbridge to ward off external threats. To promote the security and prosperity of our citizens and to safeguard our democracies, we will manage interdependence, with all the opportunities, challenges and fears it brings about, by engaging the wider world.'[3] This notion was echoed by an EU policymaker, who emphasized that 'it is not that we are trying to create an island called Europe [and] separating ourselves from the others' (Interviewee A, 2021).[4] Thus, rather than engaging in 'geopolitical battle[s]'

[2] Interviewee C, interview by author, virtual (online video), March 12, 2021.
[3] European Union, "Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy," 17.
[4] Interviewee A, interview by author, virtual (online video), March 5, 2021.

(Interviewee E, 2021)[5] and fighting with others (Interviewee A, 2021),[6] the EU aspires to create partnerships to protect its values and establish rules in cyberspace (Interviewee B, 2021).[7]

Notably, the emphasis on 'sharing values' in a collaborative sense is further linked with 'universality' and 'shared responsibility'—therefore 'co-ownership'—in the context of cyber policy. CCB programmes were described as necessary for upholding and promoting values in global cyberspace—which were described as 'not European values' but *universal* values. Using the example of privacy, one EU official acknowledged that, while people conceive of privacy as a 'European invention', the concept is in the 1948 Universal Declaration of Human Rights, which makes it universal.[8] Furthermore, while Europe is described to provide the bulk of assistance for achieving these values to third countries (and not vice versa), there was nevertheless the *shared* responsibility between the EU and the country to establish common expectations and to invest in cybersecurity.[9] As one interviewee stressed, 'we don't want to have the blind followers [as in the case of China], we want to have conscious followers' (Interviewee A, 2021). [10] This notion of sharing the EU's success (e.g. in terms of 'bringing enlightenment to others' or 'help running out of Europe') is similarly reproduced by official speeches, in the language of 'exporting Europe's stability' and the European model as 'inspiring others.'[11] Overall, such a narrative creates the impression that the EU is not only a valuable and desirable partner, but the European model *itself* is universally desirable for third countries, relative to other cyber actors (Russia and China.).

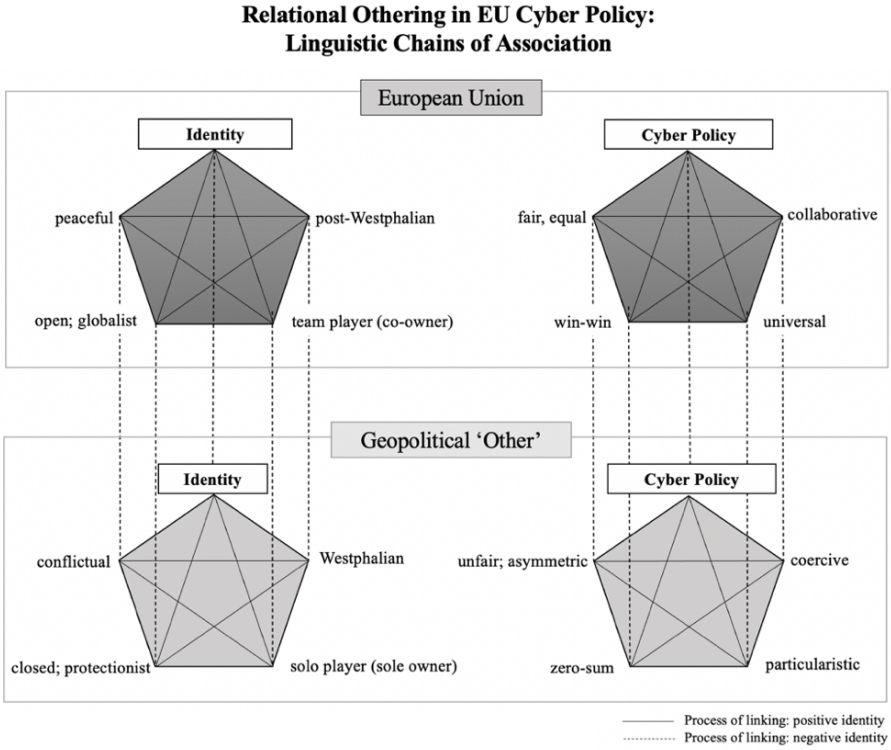
Furthermore, while help to uphold such values is 'running out of Europe' in CCB programmes with third countries, there is nevertheless the *shared* responsibility between the EU and the country to establish common expectations and to invest in cybersecurity. As one interviewee stressed, 'we don't want to have the blind followers [as in the case of China], we want to have conscious followers' (Interviewee A, 2021).[12] This sense of sharing the EU's success (e.g. in terms of 'bringing enlightenment to others' or 'help running out of Europe') raised by interviewees in various ways is similarly reproduced by official speeches, in the language of 'exporting Europe's stability' and the European model as 'inspiring others'[13] which creates the impression of the EU as a valuable and desirable partner, but the European model *itself* as *universally* desirable.

Creating positive linkages with the terms 'peaceful', 'open', 'post-Westphalian', and 'team player' reproduces previously established narrative constructions about the EU's identity as a political actor, linkages that it has cultivated in other policy arenas (namely in enlargement and security). Scholars have demonstrated that the EU's tendency to describe its enlargement policies and external relations projects in non-geopolitical terms—and to eschew politics more broadly—has been a longstanding discursive trend.[14] As one EU policy expert asserted, the EU has a 'long history' of transforming its geographical neighbourhoods, which is geopolitical, 'but never really …thought of it that way' (Interviewee C, 2021).[15] As expressed by this expert, the EU's discursive pattern of geopolitical othering nevertheless comes into tension with the inherently geospatial nature of the EU's expansionary and extraterritorial logics of security.

---

[5] Interviewee E, interview by author, virtual (online video), March 25, 2021.
[6] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[7] Interviewee B, interview by author, virtual (online video), March 11, 2021.
[8] Interviewee E, interview by author, virtual (online video), March 25, 2021.
[9] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[10] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[11] Juncker, "State of the Union 2018: The Hour of European Sovereignty."
[12] Interviewee A, interview by author, virtual (online video), March 5, 2021.
[13] Juncker, "State of the Union 2018: The Hour of European Sovereignty."
[14] Cadier, "The Geopoliticisation of the EU's Eastern Partnership"; Nitoiu and Sus, "Introduction: The Rise of Geopolitics in the EU's Approach in Its Eastern Neighbourhood"; Diez, "Europe's Others and the Return of Geopolitics"; Browning, "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War.'"
[15] Interviewee C, interview by author, virtual (online video), March 12, 2021.

As I have demonstrated above, EU policy discourses frequently draw upon established characteristics of the EU's identity to explain its approach in cyberspace—particularly the notions of itself as peaceful, a team player, open, and post-Westphalian. Reproduced over time, this process provides further chronological stability and coherence in its self-representation, therefore imbuing its self-narrative with further credibility and legitimacy. Visualized below (as displayed in Chapter VI).



Appendix 3.3 – Ipsos Poll on Sovereignty Results (2020)

Visual representation (taken from original survey) of the spread of concepts linked to sovereignty, grouped by respondents' nationality. Respondents answered the following question: 'Which of the following words are spontaneously brought to mind by the term sovereignty? First? Second?'[16]

IN %, IN TOTAL	ALL COUNTRIES	FRANCE	GERMANY	ITALY	SPAIN	POLAND	ROMANIA	LATVIA	SWEDEN
Independence	42	31	63	22	20	65	55	72	47
Power	37	51	23	46	54	9	41	15	22
Self-determination	34	22	53	25	20	40	22	42	62
Nationalism	31	43	7	58	43	6	32	14	20
Freedom	28	15	35	13	27	61	30	45	34
Protectionism	16	26	6	26	17	5	9	4	11
Protection	13	13	13	10	19	13	12	8	4

Total exceeds 100 because two answers are possible

[16] Fondation Jean-Jaurès and Friedrich-Ebert-Stiftung, "Survey on European Sovereignty Carried out by Ipsos on Behalf of the Fondation Jean-Jaurès and the Friedrich-Ebert-Stiftung."

Appendix 4 – List of Primary Textual Sources Cited*

Organized by year of publication

**Sources listed below (51) do not comprise a complete list of all textual sources analyzed as part of the author's research process, only the sources cited in the text of this dissertation. This list includes speeches and interview transcripts.*

2003	Secretary General/High Representative. A Secure Europe in a Better World: European Security Strategy, Pub. L. No. PESC 787 (2003). https://data.consilium.europa.eu/doc/document/ST-15895-2003-INIT/en/pdf.
2005	Council of the European Union. *Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems*. Official Journal of the European . L 69 (2005): 67–71.
2007	European Parliament. *European Parliament resolution of 24 May 2007 on Estonia (2007).* https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0215+0+DOC+XML+V0//EN.
	NATO Cooperative Cyber Defence Centre of Excellence. "2007 Cyber Attacks on Estonia," 2007.
2009	European Commission. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection. Brussels, 2009.
	Zanders, Jean-Pascal. "Cyber Security: What Role for CFSP?" *European Union Institute for Security Studies*. Brussels, 2009.
2010	European Union Committee. "Protecting Europe against Large-Scale Cyber-Attacks." *House of Lords Publications*. London, 2010.
	European Commission Communication. *A Digital Agenda for Europe*. Brussels, 2010. ttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.
	European Organization for Security. "Towards a Concerted EU Approach to Cyber Security," 2010. http://www.eos-eu.com/Files/Cuber-policy-docs/EOS_ICTWG_CyberSec_v5%200.pdf.
	European Commission. Standard Eurobarometer: *EUROBAROMETER 74 AUTUMN 2010 INFORMATION ON EUROPEAN POLITICAL MATTERS REPORT*. Brussels, 2010. http://ec.europa.eu/public_opinion/index_en.htm.
2011	European Commisssion. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection 'Achievements and next Steps: Towards Global Cyber-Securrity.* Brussels, 2011.
	European Commission. "Eurobarometer Survey on Internal Security : The Economic Crisis and Terrorism Top the Agenda." *Memo*, no. November (2011).

2013	European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013. https://doi.org/10.4271/2010-01-1021.
	Special Eurobarometer. "Special Eurobarometer 404 Cyber Security," 2013. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf.
2014	European Union. *Association Agreement between the European Union and Its Member States, of the One Part, and Ukraine, of the Other Part*. Official Journal of the European Unio*n* L–161, no. 2014-02–29 (2014): 1–2137. https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf.
	Barroso, Jose Manuel Durao. *European Commission 2004 – 2014: A Testimony by the President with Selected Documents*, 2014.
2015	European Commisssion. *The European Agenda on Security*. Brussels, 2015. 1–21. https://doi.org/10.4324/9780429465918-2.
	Council of the EU. *Council Conclusions on Cyber Diplomacy*. Brussels, February (2015): 1–13. http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.
	European External Action Service. *Food-for-Thought Paper: 'Countering Hybrid Threats'*. Brussels, May (2015): 8. http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15. pdf.
2016	European Commission. "Action Plan 5G for Europe - Staff Working Document." Brussels, 2016.
	Politico-Military Group. "Six Monthly Report on the Implementation of the Cyber Defence Policy Framework." Vol. 2016, 2016.
	European Union. *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy.* Brussels, 2016, 1–56. http://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf.
	General Secretariat of the Council. *Council Conclusions: Mainstreaming Digital Solutions and Technologies in EU Development Policy.* Brussels, 2016.
	Mogherini, Federica. "Speech by HR/VP Mogherini at the EUISS Annual Conference, Towards an EU Global Strategy-The Final Stage ," April 22, 2016.
	European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *Joint Framework on Countering Hybrid Threats: A European Union Response.* Brussels, 2016.
	European Parliament. *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,* Pub. L. No. L 194/1, Official Journal of the European Union 58 (2016). https://doi.org/10.2307/j.ctt1xhr7hq.20.
	Council of the EU Presidency. Cyber Capacity Building: Towards a Strategic European Approach.

Brussels, 2016. https://www.statewatch.org/media/documents/news/2016/jul/eu-council-cyber-capacity-building-8732-1-16.pdf.

2017 European Commission. *COMMISSION STAFF WORKING DOCUMENT Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy.* Brussels, 2017.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU. JOIN(2017) 450 Fina*l. Brussels, 2017.

European Commission. *REFLECTION PAPER ON THE FUTURE OF EUROPEAN DEFENCE.* Brussels, 2017. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0315.

2018 Council of the European Union. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL: Establishing the European Defence Industrial Development Programme Aiming at Supporting the Competitiveness and Innovation Capacity of the Union's Defence Industry*. SN 2717/18, no. Brussels, (2018): 1–37.

European Commission. *ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018. Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries*. Brussels, 2018.

European Commission. *Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Proposal for a Regulation of the European Parliament and of the Council. COM(2018) 630 Final*. Brussels, 2018.

General Secretariat of the Council. *EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018).* Brussels, 2018.

Juncker, Jean-Claude. "State of the Union 2018: The Hour of European Sovereignty." European Commission, 2018. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en_0.pdf.

2019 European Commission. *COMMISSION RECOMMENDATION of 26.3.2019 Cybersecurity of 5G Networks.* Brussels, 2019. https://doi.org/10.4018/978-1-7998-7708-0.ch029.

European Commission. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL Twentieth Progress Report towards an Effective and Genuine Security Union. *Official Journal of the European Union*. Brussels, 2019.

European Parliament. *Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them.* Strasbourg, 2019.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN*

	COUNCIL AND THE COUNCIL EU-China – A Strategic Outlook. Brussels, 2019.
	NIS Cooperation Group. "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks." *European Commission*, 2019. https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.
	Borrell, Josep. Interviewed by Weiler, Joseph. "Europe Must Learn Quickly to Speak the Language of Power." *EJIL: Talk! Blog of the European Journal of International Law*, October 29, 2020. https://www.ejiltalk.org/europe-must-learn-quickly-to-speak-the-language-of-power-part-i/.
2020	European Commission. *A New Industrial Strategy for Europe. COM(2020) 102 Final*. Brussels, 2020, 1–16. https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-
	General Secretariat of the Council. *Shaping Europe's Digital Future - Council Conclusions*. Brussels, June 9, 2020.
	European Commission. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's Digital Future*. Brussels, 2020.
	European Commission, and High Representative of the Union for Foreign Affairs and Security Policy. *JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade. Brussels, 2020.* https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade.
	European Court of Auditors. "Audit Preview: Implementing Secure 5G Networks in the EU and Its Member States," 2020.
	European Court of Auditors. "The EU's Response to China's State-Driven Investment Strategy," no. 0 (2020).
	Borrell, Josep. "Cyber Diplomacy and Shifting Geopolitical Landscapes ." European External Action Service, September 14, 2020. https://eeas.europa.eu/headquarters/headquarters-homepage/85069/cyber-diplomacy-and-shifting.
	European Commission. "Secure 5G Networks : Questions and Answers on the EU Toolbox," Brussels, 2020. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.
*2021***	Council of Europe, European Union. "CyberEast." Council of Europe, 2021. https://www.coe.int/en/web/cybercrime/cybereast.
	European Commission. *5G Action Plan : Shaping Europe's Digital Future*. Brussels, March 9, 2021. https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan
	***2021 sources are dated in accordance with the date the webpages were last accessed by the author.*