Virtually inconceivable: Geopolitics, capacity, and sovereignty claims in the digital domain

Julia Carver

Nuffield College

Thesis submitted in partial fulfilment of the requirements for the degree of DPhil in International Relations in the Department of Politics and International Relations at the University of Oxford

Trinity Term 2025
Word count: 83497

Table of Contents

List of Tables

List of Figures

Thesis abstract

Once virtually inconceivable, cyberspace has emerged as a new arena for global geostrategic competition. With its complex territoriality and evolving technological features, this domain has challenged traditional theories of geopolitics and sovereignty in international relations (IR). Dominant accounts of 'cyber-geopolitics' have struggled to explain the European Union's (EU) striking emergence as an explicitly 'geopolitical actor' in search of 'digital sovereignty' in and through cyberspace. More broadly, IR literature has undertheorized the relationship between geostrategic behaviour, ontological security, and the capacity to project power in and through cyberspace. As a consequence, the overlapping developments of geostrategic competition in cyberspace and the EU's emergence as a geopolitical actor remain poorly understood.

This integrated thesis examines the emergence, drivers, and characteristics of the EU's geostrategic behaviour in and through cyberspace within the broader context of global competition. Departing from a critical ontological approach, this dissertation analyzes over 150 primary source documents between 2009-2024 and two dozen elite interviews conducted by the author. Empirically, the three articles examine the overlooked geostrategic dimension to American, Chinese, and EU-funded capacity building initiatives in Africa; the opaque relationship between European digital sovereignty objectives and significant EU cybersecurity policy changes; and how ontological security drives have underpinned the EU's geostrategic approach to cyberspace. Altogether, this thesis constitutes one of the first studies to integrate EU external action towards digital sovereignty, cyber capacity building, and ontological security in cyber geopolitics.

Contributing to IR scholarship on (cyber)security studies, the dissertation reveals how contemporary geostrategic competition has been characterized by actors' efforts to build greater capacity in and through cyberspace by deploying a variety of hard (infrastructural) and soft (regulatory) tools. Counter to dominant accounts, I argue that this

behaviour, particularly in the EU context, has been mediated by actors' ontological security drives, not only material security concerns. In our rapidly evolving, digitalizing, and unstable international order, understanding these foundations of contemporary geostrategic behaviour is of critical importance for IR.

List of common abbreviations in this thesis	
CC TT	European Commission Competence Centre on Technology Transfer
CERT	Computer Emergence Response Team
CFSP	Common Foreign and Security Policy (European Union)
CITCC	International Telecommunications Construction Corporation (China)
CSDP	Common Security and Defence Policy (European Union)
DCCP	Digital Connectivity and Cybersecurity Partnership (United States)
DG CNECT	Directorate-General for Communications Networks, Content and Technology (European Commission)
DG INTPA	Directorate-General for International Partnerships
DG NEAR	Directorate-General for Neighbourhood and Enlargement Negotiations (European Commission)
DTA	Digital Transformation with Africa Initiative (United States)
D4D	Digital for Development (European Union initiative)
EaP	Eastern Partnership (European Union initiative)
EEAS	European External Action Service
EP	European Parliament
EU	European Union
EUCS	European Union Cyber Strategy (2013)
EUGS	European Union Global Strategy (2016)
GFCE	Global Forum on Cyber Expertise
GLACY+	Global Action on Cybercrime Extended (GLACY)+
HR/VP	High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission
ICT	Information and Communication Technology
JHA	Justice and Home Affairs (European Union)
NATO	North Atlantic Treaty Organization
OECD	Organisation for Economic Co-operation and Development
PRC	People's Republic of China
UN	United Nations
UN GGE	United Nations Group of Governmental Experts
US	United States
USAID	United States Agency for International Development

Thesis acknowledgements

This thesis was written across three continents, two universities, and four Oxford colleges. Those places are occupied by many people to whom I am deeply grateful.

Foremost, this thesis would not have been possible without the continuous support of my supervisors, Robert Johnson and Dominic Johnson. I met Rob in the first month of arriving in Oxford. Over six years, two degrees, and one pandemic, Rob took me under his wing, supporting me at my lowest periods during the DPhil 'pushing me off the deep end' when I needed it the most. Rob's belief in my ideas dared me to 'dream big' in many ways. He shaped my understanding of research and its application to policy practice, as well as stoking a passion for science and technology. I am very grateful for Rob's mentorship, his generosity, and steadfast supervision throughout both the MPhil and the DPhil degrees. I will sorely miss his 'warm regards', our laps around Christ Church meadow, and the welcoming office of CCW. I am also deeply grateful for Dominic's pragmatic advice, thoughtful feedback, and deep knowledge of IR, which were integral for shaping the wider scope of the project and navigating the requirement of the DPhil degree. He brought a crucial perspective to the thesis and helped me to navigate the new field of IR (a transition from my previous degrees). His support, detailed comments, and good humour throughout challenging periods of the degree were invaluable to my dissertation.

Throughout the DPhil, Nuffield College was a crucial support system for me. I am so grateful for the constant support and understanding from Eleni, Nuffield's Senior Tutor, and for the necessary financial support provided by the College, as well as the UKRI/ESRC to fund my DPhil degree. Nuffield, in tandem with CCW, supported my development of a Cyber Strategy and Technology working group, which I undertook for the first three years of the degree. This working group generated many fascinating discussions about cybersecurity, digital strategy, and its relationship to European policy issues, and I am very grateful to the participants for sharing their insights and knowledge. These discussions, which also occurred more broadly across the University, formed the backdrop and motivation of this research.

At Pembroke College, the CCW 'family'—including Maria, Liz, Leanne, and Will, as well as the cohorts of CCW Fellows—was an indispensable part of my daily DPhil life. They truly opened my eyes to the practice of international relations and international security and they demonstrated to me the importance of thinking beyond the 'ivory tower'. I am particularly grateful to Will for his mentorship, candid advice, witty remarks, and our post-seminar debriefs at the Bear.

I must also thank many dear friends across the University who were indispensable for my time at Oxford. First, I am so grateful to have the companionship and support of my friends in the DPIR, with whom we wrote our MPhil dissertations, completed the taught components of the degree, and spent many enjoyable days and nights outside of the department together. While most of us embarked on our own DPhil thesis journeys, with Scott, Mihnea, Katarina, Tiphaine, and Rachel, I never felt that I was striking out alone. I could always count on them for their support, love, and their brilliant ideas. I am also grateful to Sam, Ben, and Claas for their social and intellectual company during the DPhil, during which we spent many enjoyable hours exploring topics somewhat adjacent to our own dissertation research. More broadly, thank you to my IR cohort and DPIR colleagues for providing me with feedback at several IR Colloquia, which were especially helpful for the early drafting of the papers. A big thank you to Lis, Alejandro, Haydn, Salma, Kayla, Taylor, and John for inspiring me academically and professionally. And thank you to my friends from Teddy Hall and beyond, including Ben, Julie, Jochem, Antonin, Raggy, and Fernando, for passing many days with me playing croquet, painting with Bob Ross, and enjoying Oxford's many pubs. I am especially grateful to Jenny Crewe, who went above and beyond for all students in the DPIR (including me) and was constantly striving to make the department a fruitful place of learning.

This DPhil has also been shaped by a three-year stint as a Lecturer at Magdalen College, where I spent many happy days—often with Bethan—at the OKB, the New Building, and around Addison's Walk. There, I was able to delve further into IR and Politics topics with many bright students, who have spurred many reflections about power and global affairs. My students inculcated within me a love for teaching and learning about IR, and their own learning journeys inspired me to be more 'curious' and gave me much-needed energy which has undoubtedly shaped my own research. Furthermore, I am very grateful to Paul Billingham, Magdalen's Senior Tutor of Politics,

for believing in my teaching and for enabling me to grow as both a DPhil student and as a Tutor throughout my three years there.

At Oxford, I also benefitted greatly from the leadership, support and understanding of my colleagues at the Global Cyber Security Capacity Centre at the Department of Computer Science. There, I was welcomed very warmly into the GCSCC research team, and I learned much more about the practice of cyber capacity building through various country perspectives, and its associated challenges and opportunities. I am very grateful for the flexibility, patience, and kindness of Michael and Sadie, my brilliant supervisors. Thank you for trusting in me to work on some very exciting projects, and also for your flexibility throughout my thesis writing-up phase. I further appreciate the support from my colleagues and friends, Ingrid, Patricia, Louise, and Joe, who always cheered me on.

Throughout my degree, I was also privileged to present my work at multiple conferences, panels, and roundtables. The feedback and discussion which emerged from these opportunities, including BISA, ISA, EISS, NATO CyCon, the Hague Program Annual Conference on International Cybersecurity, and the ECPR Standing Group on the EU, was invaluable to my project. Particularly, Timo Seidl, Anke Obendiek, Sebastian Heidebrecht, and Gerda Falkner invited me to publish my research paper in a special issue in *The Journal of European Public Policy*. This process provided me with much-needed support, confidence, and encouragement to produce my first ever journal publication (Chapter 5 of this thesis). Similarly, I would like to thank Myriam Dunn Cavelty and the editing team at *Contemporary Security Policy* for their assistance and support in publishing my research, which yielded valuable feedback and shaped the article (Chapter 4). Finally, I am very grateful to my colleagues in friends in three research networks and centres: Virtual Routes, the European Initiative on Security Studies, and SST-CCW at Oxford, who have constantly supported my growth as a researcher, including Max Smeets, James Shires, Hugo Meijer, and Moritz Weiss.

Moreover, I wrote the final leg of the thesis while beginning a research position at the University of Leiden, and I would not have been able to make it to the finish line without their flexibility and support. I am very grateful to my current colleagues at the University of Leiden, particularly Professors Dennis Broeders, Bibi van der Berg, and friends in the Hague Program research team for their patience and encouragement.

Across the Atlantic, back home, I am thankful for my steadfast friends– Sandy, Meg, Emily, Aly, Siena, and Lauren, who have been so patient with me throughout my DPhil journey and consistently provided their support and love, even when I dropped off the map for a conspicuous amount of time (!). Sandy, thank you especially for your constant love and unwavering belief in me, and for your very thoughtful cards, which always arrived overseas at the most crucial 'low points' in my thesis writing and motivated me to keep going.

Finally, and most importantly, this dissertation would not have been possible without the support of my family, particularly my partner, Thijs, my parents, Dan and Pam, and my sister, Katrina. Since the first day I stepped foot in Oxford, Thijs has supported me every step of the way. From evening walks around Headington Hill park, playing cards at the Star, cycling trips, bird watching in the Kidneys, to Welsh weekend camping trips with Djungel, his companionship enabled me to thrive as a researcher and a person. His unconditional support, even-keeled approach to life, and his belief in me enabled me to keep going when it felt impossible. And above all, without my parents and my sister, I would not have boarded the plane to England in 2019, or even contemplated Oxford at all. My family's strength and integrity have constantly served as an inspiration for me to 'do *my* best' and to enjoy the wider aspects of life—including nature, friends, family, fictional books, and English gardens. In the face of many recent challenges, they have modelled true strength and resilience, and I am grateful to them beyond words for their unwavering support, consideration, and understanding. Thank you to Dan, Pam, and Katrina for giving me the strength to pursue my ('Redwall') dreams and to overcome my fears. I owe it all to you.

This work was supported by Economic and Social Research Council [grant number ES/P000649/1]; and by Nuffield College, University of Oxford.

Chapter 1: Introduction

‘Cyberspace does not lie within [government] borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.’– *John Perry Barlow, 1996*

On 14 September 2020, Josep Borrell, the serving diplomat of the European Union’s External Action Service, stepped up to give the keynote address to the EU Cyber Forum. Before European governments, the private sector, and civil society, he declared that ‘cyber issues are geopolitical in nature and have a strong security dimension,’ (European External Action Service, 2020). 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 Sino-American 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’; and the ongoing ‘battle of narratives’ in the digital domain (European External Action Service, 2020).

Borrell’s observations reflect an increasingly fraught global strategic landscape, whereby cyberspace has emerged as an arena of geostrategic competition and territorial claims (see also Betz & Stevens, 2013). In this environment, ‘traditional’ powerful geopolitical competitors, such as the United States (US), China, and Russia, have often eschewed direct military confrontations in favour of ‘resolv[ing] their quarrels primarily in other planes of conflict’ (Kello, 2022, p. 10). For example, Washington’s 2024 *International Cyberspace & Digital Policy Strategy* laid out the ‘pressing and high stakes’ challenges accompanied by digital transformation, emphasizing that ‘The geopolitics of cyberspace are competitive and complex’ (2024, p. 11). Beyond the transatlantic context, cyber activities comprise a key facet of contemporary geopolitical competition for Russia and China,

enabling state actors to compete below the threshold of traditional conflict (Buchanan, 2020).

Rather than emerging as an era of 'peace', international relations in the post-Cold War context has been characterized by persistent competition (Kello, 2022; Buchanan, 2020) and the decline of the liberal international order (Flockhart, 2020). As Josep Borrell acknowledged in his 2020 remarks,

> 'We know the world is becoming more digital, but also more state-driven […] In short, our security environment is getting worse. Everywhere we look, we see rivalries, especially between the US and China, with technology as a major fault line and cyber as the new domain,' (European External Action Service, 2020).

Yet, such competition has not been limited to traditional nation state actors or their sponsorship of hacker groups (Sukamar et al., 2024). Indeed, other powerful global competitors have advanced geopolitical and sovereigntist claims in and through cyberspace. Strikingly, the European Union, which has long framed its *raison d'être* in diametrical opposition to geopolitics (Guzzini, 2012), has advanced its own geostrategic ambitions underneath an agenda of 'digital sovereignty'. Under this new approach to the 'Digital Decade', cybersecurity is considered a critical enabler of the Union's geostrategic goals (Bellanova et al., 2022; European Commission, 2022; General Secretariat of the Council, 2022).

Critically, while global politics have become increasingly shaped by digital technologies (Acemoglu & Johnson, 2023), IR scholarship has yet to fully understand or explain the co-evolution of cyberspace and contemporary geostrategic behaviour, particularly in the European Union. Given these developments, this dissertation is motivated by the overarching research question:

> What explains and characterizes geostrategic behaviour in and through cyberspace, and what are the implications for the nature of sovereignty and geopolitics in the digital age?

There are pressing academic and policy reasons to scrutinize the features and causal logics of geostrategic behaviour in and through cyberspace, particularly in the context of the EU's external action approach. Foremost, cyberspace, as a 'complex socio-technical system', has become further integrated with other policy domains and sites of power in international politics (Dunn Cavelty & Wenger, 2022, p. 2). Over the past decade, internet infrastructure—the backbone of cyberspace—has emerged as the site of weaponized (digital) interdependence and cyber espionage concerns (Drezner et al., 2021). Fears of coercion and exploitation by digital dependence have spurred African member states, for example, to underscore the relationship between cybersecurity, digital transformation, and national sovereignty (African Union, 2020). While cases of 'wiretapping' have exposed the strategic import of enjoying privileged access and/or control over networks (Drezner et al., 2021), recent cyberattacks on connectivity infrastructure—such as disrupting satellites and supply chain vulnerabilities in Europe—have also underlined the risks of cross-border digital integration (Council of the European Union, 2022; Richmond, 2019).[1]

Increasingly, geostrategic behaviour in and through cyberspace has entangled with other emerging digital technologies, including cloud computing and artificial intelligence, and issues of international political economy and development, including demand for global digitalization. These changing conditions have altered the risk calculus policymakers had applied towards liberalized technological innovation and global digital interdependence (Tan et al., 2025). Today, addressing digital dependence and strategic technological

[1]Recent examples include the AcidRain wiper (malware) attack against satellites providing coverage to Ukrainian infrastructure, and the Cloud Hopper (supply chain) attack (against managed service providers with global scope), attributed respectively to Russian and Chinese state-linked hacker groups. See Council of the European Union (2022) for the ViaSat hack, and Richmond (2019) for a case study on Cloud Hopper.

vulnerabilities have become existential concerns for governments (Von der Leyen, 2024; US Department of State, 2024; Carpenter & Hollis, 2023).

Evolving dynamics of geostrategic behaviour in and through cyberspace raise significant questions about the perceptions, power, and interests of major international actors, as well as the uncontested role of the nation-state as the 'sovereign' in the digital age. In this regard, scholars have argued that contemporary geostrategic behaviour in and through cyberspace is not merely 'old wine in new bottles': it challenges the classical 'war/peace' binary in international affairs (Kello, 2017) and it complicates traditional notions of territorial sovereignty (Balzacq & Dunn Cavelty, 2016). For the EU, for example, digital sovereignty claims are not only complicated by potentially competing or 'pooled' sovereignty claims (Moravscik, 1998), but by the complex structural features of cyberspace. Not only does cyberspace's transnational, networked architecture challenge traditional parameters of sovereign territoriality, but its networked digital backbone is owned and/or operated by a few powerful private firms mostly headquartered in the United States and China (Pohle & Voelsen, 2021).

The prevalence of strategic competition in and through cyberspace—and its complications for classical conceptions of territoriality—could mark a transformation in how policymakers approach geopolitics and sovereignty as strategic concepts in the digital age. As a 'sociotechnical system' (Dunn Cavelty & Wenger, 2022, p. 2), cyberspace cuts across the 'digital technology stack', imbricating with issues of artificial intelligence, network security, digital infrastructure, and virtualization (e.g. in cloud computing).

The sociotechnical nature of cyberspace presents opportunities for various global actors to reconfigure the way in which geopolitics and sovereignty are imagined and practiced in the digital age. Changing strategic approaches to 'cyber geopolitics' and their integration into wider foreign policy objectives could encourage a new dominant form of

geopolitical competition in global politics premised upon networked power, not geographic territorial control. Studying the co-constitutive relationship between cyberspace and geostrategic behaviour, then, is crucial for understanding how geopolitics and sovereignty are practiced in contemporary global politics, and their potential future consequences.

Critically, geostrategic competition in and through cyberspace has not only become a challenge for international relations scholarship (as I will detail in the coming pages), but it is a real and pressing policy issue. For practitioners, developing cyber strategy is dogged by problems with conceptualizing the scope and the nature of cyber insecurities and their application to international law. Policymakers have also struggled to keep pace with rapid technological changes, including the increasing sophistication of cyber capabilities, whilst balancing economic, political, and social pressures for greater digitalization across a variety of critical national sectors (Gomez & Whyte, 2021). Simply put, the reality is that 'managing cyber insecurities continues to be a most challenging governance issue in contemporary politics,' (Dunn Cavelty & Wenger, 2022, p. 1). As governments continue to pursue digital transformation in an increasingly uncertain global environment, gaining a deeper understanding of the emergence, drivers, and characteristics of geostrategic behaviour in and through cyberspace has become a critical foreign policy issue. These dynamics constitute the wider backdrop for this thesis.

The remainder of this introductory chapter provides an overview of the research agenda, motivation, key questions and conjectures, and core definitions for the thesis. This sets the stage for a comprehensive review of the literature (in Chapter 2) and an outline of the theoretical foundations of the thesis (in Chapter 3). Next, this chapter summarizes the three substantive research articles comprising the thesis (Chapters 4-6), and their overall contributions, as a foreshadowing to the conclusion chapter of the thesis (Chapter 7). Before I delve into the specific research objectives of the thesis, it is important to clarify how I will

approach ‘cyberspace’, ‘sovereignty’, and ‘geopolitics’ as concepts, and their related challenges and tensions in existing IR scholarship.

Geostrategies in and through cyberspace as ‘wicked problems’

Cyberspace’s convergence with geopolitical behaviour and its complex entanglement with both the cybersecurity and foreign policy fields is a particularly pressing and ‘wicked’ problem for IR scholarship; a problem that is ‘not only difficult to solve, but difficult to define’ (Stevens, 2023, p. 8). While Chapter 2 provides a comprehensive overview of various conceptual approaches to cyberspace in scholarship and practice, *cyberspace* can be broadly understood as ‘a complex socio-technical system’ whereby technologies and politics are considered inseparable from each other (see Table 1.1 below; Dunn Cavelty & Wenger, 2022, p. 2; see also Slayton, 2016). As exemplified by ‘cybersecurity’ (or ‘cyber security’), the term ‘cyber’ often occurs as a concatenation to many basic concepts in international relations,[2] including ‘power’, ‘the state’ and ‘society’, as evidenced by concepts such as ‘cyber power’, ‘cyber conflict’, and ‘cyberattack,’ (see for example Nye, 2011; Branch, 2021).

Networked layers of cyberspace	***Description***	***Characteristics***
Hard infrastructural layer	Hardware components which form the architecture of cyberspace – ICT/ telecommunications infrastructure (e.g. TV towers), computers, submarine cables, etc.	▪ Material / physical
Technical / informational layer	Software – social media, domain names, IP protocols, social media, search engines, containing information	▪ Informational: primarily virtual, with material elements

[2] Drawing upon Berenskoetter (2017), I use the term ‘basic’ concepts in the Koselleckian sense; that is, as fundamental concepts of a political system that ‘we cannot do without’ (p. 157). In the domain of international relations, basic concepts include ‘power’, ‘attack’, ‘war’, and ‘security’ (pp. 153, 157).

Human layer	Human participants– be they customers/consumers, corporate actors, government officials, computer users	▪ Social (physical and virtual) ▪ Individual/ ideational (immaterial)

Table 1.1. Author's conception of networked layers of cyberspace, synthesized from literature (see also Chapter 2).

As I explain in Chapter 2, 'geopolitics' is fundamentally about 'representations of space and the spatial practices underpinning world politics' (Ó Tuathail, 1998, p. 17); a form of statecraft which is premised upon the political, social, and economic relationship between space, power, and strategy (Agnew & Corbridge, 1989; see also Dodds, 2019). Drawing from critical geopolitics approaches, I understand geopolitics not as a given variable but as a *question*; as a form of knowledge production (Kuus, 2014; see also Ó Tuathail & Agnew, 1992). Approaching geopolitics through such an analytical perspective, I contend, enables us to critically examine actors' *geostrategic behaviour*—that is, how and why actors have adopted particular *geostrategies* in their practical approaches towards cyberspace. As I introduce over the next page, this dissertation is largely concerned with two related geostrategic practices in and through cyberspace: *geopolitical* and *sovereigntist behaviour*.

Aside from scrutinizing actors' purposive 'geostrategies', adopting a critical geopolitics analytical perspective reveals how mainstream IR scholarship, particularly security studies, have associated *cyber-geopolitics* with a particular 'modernist' approach to physical geography and the projection of power (Dunn Cavelty, 2018; McCarthy, 2015). According to modernist accounts of geopolitics, states advance 'grand international visions' (Kuus, 2011, p. 1141) and pursue expansionist territorial goals (Guzzini, 2012). In the 20th century, for example, influential (modernist) Anglo-American approaches to land and sea power emphasized variables such as the state's territorial boundaries and its positioning vis-à-vis geographic areas of strategic importance (e.g. key trade routes or corridors) and the development of new technologies which could transform the state's capacity to traverse

geographic terrain and thus reshape political boundaries, such as railway infrastructure (Klinke, 2021).

Relatedly, *sovereignty* is a core politico-legal concept establishing the basis of rule for states in the international system (Krasner, 1998), encapsulating both an internal and external dimension: the assertion of exclusive authority over a bounded socio-political space—that is, over a digital and/or cyberspace—and the legitimisation of this claim through mutual recognition (Thomson, 1995). Accordingly, sovereignty can be understood as both a (discursive) representation of space—that is, a 'concept', 'naming practice' and/or 'geographical code used to talk about and understand spatial practices' (Agnew and Corbridge 1995, p. 7)—*and* as a (material) spatial practice underpinning world politics. 'Digital sovereignty', then, can be understood to broadly encapsulate the expression of legitimate authority and control over a bounded socio-political space—that is, over a digital and/or cyberspace (Thomson, 1995).

As I demonstrate in Chapter 2, the environmental features of cyberspace complicate popular modernist understandings of geopolitics, which are concerned with a state's material projection of power over and across sovereign (physical) territorial space (Dodds, 2019; Ó Tuathail, 1998, pp. 23). Compared to other 'physical' domains, cyberspace has a fluid, complex, and tenuous link with 'Westphalian geography', as it encompasses weak locational factors, networked hierarchies in which power is diffused rather than transferred, and greater access for non-state actors to exert power (Taddeo, 2017; Nye, 2017). Furthermore, the digital infrastructure which comprises the physical backbone of the internet—such as submarine cables and ICT infrastructure—elides neat territorial boundaries and state control (see for example Gjesvik, 2023; Lehdonvirta, 2022; Moiso & Paasi, 2013). As I explore in this thesis, many global actors have divergent ontologies about the boundaries of cyberspace

as a domain, including between key cyber players (viz. the US, China, Russia, EU), further raising questions about 'fixed geography' in actors' strategic imaginaries.

These characteristics disrupt popular classical assumptions about international relations, whereby the state, sovereignty, and the military are territorially packaged into 'a bordered power container,' (Giddens, 1985). In a similar vein, the complexities of territoriality in and through cyberspace also complicate the expression and operationalization of traditional and/or state-based sovereignty claims as a form of Westphalian 'state-force-territory relation,' (Barkawi, 2016).

Strikingly, while cyber-IR theorists have long recognized the challenges of applying classical IR theory to cyberspace (see for example Kello, 2013; Slayton, 2016), realist approaches in security studies have tended to rely upon fixed assumptions of territory and capabilities to make sense of contemporary geopolitical competition in and through cyberspace (Lambach, 2020) or engaged in debates about cyber power premised upon these assumptions (Slayton, 2016). Alternatively, networked-based conceptions of cyber-geopolitics have largely emphasized the uniqueness of cyberspace (as distinct from other domains) and decentralized relations of power in cyberspace, often eliding the political consequences of emerging network *asymmetries* across the technology stack (Lambach, 2020; Pohle & Voelsen, 2022). Moreover, both classical and 'networked' accounts of cyber-geopolitics have yet to fully explore the co-constitution of cyberspace and geostrategic thinking and practices over time, and in contexts beyond the classical nation state.

Second, perhaps due to the predominance of state-centric and realist approaches in mainstream cyber-IR scholarship (Dunn Cavelty, 2018), there have been few studies about the EU's development as a *distinctive* geostrategic actor in cyberspace (cf. Farrand et al., 2024). Rather, the EU has been positioned as the geopolitical 'playground' between the US and China—not a geopolitical player (Weber, 2020). The thematic foci of mainstream cyber-

IR (being the threat of force, capabilities to conduct cyberwar, and the struggle between great powers) informs the common narrative that the EU possesses weak or insufficient cyber power to entertain such ambitions (Dunn Cavelty, 2018; e.g. Sliwinski, 2014; Weber, 2020). Indeed, the EU lacks the military or intelligence capabilities to conduct cyber warfare in accordance with the conventional (realist) sense of the term. Furthermore, since the EU is not, ipso facto, a (sovereign) territorial state, it confounds explanations that accredit Westphalian-state characteristics as a *precondition* to issuing sovereignty claims in political space (Agnew, 1994; Eudaily & S. Smith, 2008).

For EU Studies scholars, too, the EU's contemporary embrace of sovereignty and geopolitical language constitutes a striking deviation 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. 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,' which holds that, the EU, under the auspices of its 'virgin birth' as a supranational organization, forswore traditional forms of geopolitics to frame itself as a post-Westphalian success story (Onar & Nicolaïdis, 2013; see also Zielonka, 2006). 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 century,' (Guzzini, 2012, p. 6).

Consequently, as I explore in Chapters 2 and 3, realist and state-centric approaches to cyberspace have been unable to adequately explain the EU's development of assertive 'EU-specific' strategic instruments and geopolitical aspirations, as distinct yet related to the foreign policies and strategies of its Member States (for a broader discussion, see Sjursen, 2011; Moiso & Paasi, 2013). Under the EU's 'geopolitical Commission', the EU has pursued

its objectives of ‘digital sovereignty’ with a budget of over €8.1 billion, which has included a host of specific provisions relating to the Union’s strategic approach to global cyberspace and/or cybersecurity (European Commission, 2025). In fact, the EU has recently been likened to the United States and China as one of three competing ‘digital empires’ (Bradford, 2023) or ‘digital hubs’ (Drezner at al., 2021) in global affairs, thereby pointing to its emerging potential as a significant geostrategic actor, including in and through cyberspace. Thus, the EU’s emergence as a *sui generis* geostrategic actor exposes several relevant empirical and theoretical puzzles to cyber-IR literature on geopolitics and sovereignty in and through cyberspace.

Overall, the field has produced diverging understandings about the nature of geopolitics and the seizure of territory in cyberspace and its implications for the nature of sovereignty. These debates leave open key questions about the relationship between geography and the capacity to project power in the digital age, particularly in the case of the EU’s emergence as an avowedly ‘geopolitical actor’ in search of ‘digital sovereignty’. They also highlight the need for a greater understanding about how and why cybersecurity tools and solutions have been integrated with foreign policy, and its consequences for our assumptions about geostrategic behaviour. These broader tensions and puzzles motivate the following research gaps explored by the thesis, discussed below.

Overview of integrated thesis: Research gaps

What explains and characterizes geostrategic behaviour in and through cyberspace, and what are the implications of these dynamics for the nature of sovereignty and geopolitics in the digital age? In Chapter 2, I argue that the field has an inadequate understanding of three important aspects of geostrategic competition in and through cyberspace: 1) the EU’s emergence as a geostrategic actor; 2) the foundations of capacity as a strategic concept in

theory and its relationship to capacity building practices; and 3) the potential ontological security drivers of geostrategic competition. Exploring these gaps would shed light on several important aspects of geostrategic competition and enable us to better understand the foundations of this behaviour, offering insights for both scholarship and policymakers.

Foremost, despite the EU's established (if quixotic) role as a global security actor, mainstream cyber politics and IR literature has not comprehensively examined the Union's distinctive ambitions to become 'sovereign' actor in the cyber domain and to 'learn the language of geopolitical power' (Borrell, in Weiler, 2020). Undertaking further research on this topic would not only extend knowledge beyond the cases of traditional 'great power' activity in the cyber domain, but it would also provide the means for further challenging realist and state-centric assumptions about geopolitical competition and the exercise of cyber power in cyberspace. For the interdisciplinary field of EU studies, this research would also help to address an important (cyber-specific) gap in our understanding about EU foreign policy and the EU's (aspiring) identity as a global actor.

Second, the field's analytical focus upon cyber capabilities for explaining dynamics of geostrategic competition has overlooked the significance of 'capacity' (building) as a strategic concept in theory and practice. As I argue in Chapter 2, dominant accounts of cyber geopolitics have focused upon cyber *capabilities*, especially in the US, Chinese, and Russian state contexts, in line with realist-oriented work (see for example Buchanan, 2020; Kello, 2022; cf. Smeets, 2022). Yet, focusing upon cyber capabilities in the context of the EU's foreign policy domain is insufficient for understanding the full scope of the EU's development as a cyber actor. After all, the Union traditionally lacks competences for developing more traditional 'capabilities' (e.g. an intelligence arm and offensive/defensive cyber weapons), and it has instead engaged efforts to shape the international environment

through a variety of development assistance tools and regulatory measures linked to its digital sovereignty agenda.

Moreover, despite the pathbreaking contributions of this scholarship, dominant accounts have scarcely covered the relationship between cyber capacity building, cyber power and actors' geostrategic behaviour. This development extends far beyond the EU context. Rather, capacity building initiatives have emerged as a strategic priority across the world for both powerful and weak global actors (Collett & Barmpaliou, 2021; see also Pawlak, 2016). A plethora of states and organizations have stressed the importance of cyber capacity building as a tool of foreign policy and as a key pillar of national sovereignty (see for example United States Department of State, 2024; Ministry of Foreign Affairs of the People's Republic of China, 2016; African Union, 2020). Despite this significant development, we have a limited understanding about how and why actors have increasingly linked 'cyber (in)capacity' to digital sovereignty claims and practices (see for example, Madiega, 2020; African Union, 2020). Altogether, there remains a sore need for further research about the evolving relationship between geostrategic behaviour, cyberspace, and cyber 'capacity', as well as greater theoretical scrutiny about the distinction(s) between 'cyber capacity' and 'cyber capabilities' in theory and practice. By exploring these issues, we can gain a wider and deeper understanding of the nature and characteristics of geostrategic competition in the digital age, supplementing analyses of nation state capabilities.

Third, while cyber-IR scholarship has established a strong precedent for exploring ontological security dimension of cybersecurity decision making (as I discuss in Chapters 2 and 6), the field has largely shied away from examining this relationship in the context of geostrategic competition (cf. Lupovici, 2023). Elsewhere, ontological security conditions are theorized to underpin an actor's agency and sense of existence in the world—that is, their

capacity to act in time and space, in relation to others (Krickel-Choi, 2024; Mitzen, 2018). Furthermore, ontological security drives have been theorized to condition states' foreign policy behaviour (Subotić, 2016), including their engagement with geopolitical and/or spatial concepts (Eberle & Daniel, 2022). Foregrounding the potential ontological security dimension to geostrategic behaviour in the context of cyberspace would generate further analytical tools for exploring the immaterial and ideational dimensions of cybersecurity decision making. It would also overcome the limitations of materialist and state-centric accounts of cyber-geopolitics, which have been unable to explain the EU's development as a geostrategic actor.

To redress these gaps, this integrated thesis examines the emergence, drivers, and characteristics of the European Union's geostrategic behaviour in and through cyberspace within the context of global politics. Collectively, this dissertation serves as one of the first studies to examine the EU's evolving external action approach towards digital sovereignty and cyber capacity building, as well as the ontological security dimensions to the EU's spatial bordering practices in and through cyberspace. In so doing, all three articles in this thesis (Chapters 4-6) develop further analytical tools to explain the EU's emergence as a geostrategic actor, and they offer further empirical insights about how and why the EU has integrated cybersecurity policies and practices into its wider geostrategic agenda in particular ways. The specific objectives and contributions of the dissertation's research articles are detailed below.

Chapter outline and overview of research articles

Chapter 2 surveys IR literature on geostrategic competition, including in the context of cyberspace, and argues that critical geopolitics and constructivist scholarship jointly provide a fruitful point of departure for approaching the primary research gaps addressed by the thesis. Next, Chapter 3 lays out the study's methodological and analytical foundations,

premised upon a critical, 'ontologically' reflexive approach to geostrategic behaviour in and through cyberspace. Additionally, Chapter 3 clarifies the dissertation's scope and it provides essential background to the EU external action policy context.

The first research article, in Chapter 4, theorizes that capacity building assistance for digital development has emerged as a significant dimension of geostrategic competition in and through cyberspace. It asks: *How do powerful donors, namely the EU, US, and China, perceive capacity building assistance for digital development as shaping their strategic advantage? And which factors have shaped variation in their provision of capacity building assistance to developing states?* Examining three pathways for capacity building intervention, the chapter demonstrates how American, EU, and Chinese state-based donors have perceived capacity building assistance as enabling them to compete with each other through establishing (or strengthening) structural ties with recipients, seeking to offset the influence of rivals or project normative through providing substantive skills transfers, and/or shaping the development of governance frameworks and technical standards by providing training workshops and collaborations to local government officials. Additionally, the analysis reveals how the nature of *cyber* capacity building as a tool has evolved over time for the United States and the EU, from an emphasis on 'softer' norms and tools towards encompassing a greater scope of policy fields and infrastructural geopolitical objectives. This suggests a new approach by the US and the EU to managing weaponized interdependence and geopolitical objectives through cyberspace and/or cyber instruments.

Accordingly, my dissertation is the first to identify an influential convergence between foreign policy discourses/approaches towards cyber and digital *capacity building* and geopolitical competition. By demonstrating how capacity building assistance for digital development can operate as a tool of geopolitical, structural influence, this paper contributes to nascent scholarship on digital competition, weaponized interdependence, and geopolitical

strategy (e.g. Broeders et al., 2024), and to calls for further research on the relationship between state capacity and cyber power (e.g. Smeets, 2022). Accordingly, Chapter 4 underlines how the EU has emerged as an active geostrategic player in and through cyberspace—at least at the discursive level—by strengthening partnerships and connections with third countries and competing with both the US and China to promote its preferred norms, best practices, and connectivity projects.

Examining another key facet of the EU's geostrategic behaviour, Chapter 5 scrutinizes the relationship between European digital sovereignty discourse and policy change in the EU external action context. It addresses a significant gap in scholarship regarding how, if at all, the EU's claims to 'digital sovereignty' have shaped concrete policy developments in several cyber-relevant areas of EU external action. While the EU's discourse of 'digital sovereignty' appeared to mark a transformative shift in the EU's approach to global affairs (McNamara, 2023), it remains unclear whether this discourse has driven concrete changes to the EU's global approach to cyberspace which operationalize such ambitions. To explore this puzzle, this article asks: *To what extent has European digital sovereignty discourse driven significant changes to EU external action policies which leverage cybersecurity tools?* By examining this question, we can better understand what mediates the relationship between geostrategic ideas and their operationalization (or not) in and through cyberspace, and the EU's behaviour as a cyber actor in this context. Prior to this research, very few studies had explored how, and why, cybersecurity is mainstreamed into broader geostrategic objectives, particularly in the context of EU external action.

Drawing upon extensive archival research and two dozen elite interviews, this chapter focuses upon three significant policy changes—the Cyber Diplomacy Toolbox, the 5G Toolbox, and cyber capacity building programmes—and finds that cyber instruments have served as important enablers for operationalising Brussels' control *in practice* over the

digital domain. However, the EU's sovereigntist discourse has had an uneven and incoherent influence over the policy change process. Particularly, while European digital sovereignty discourse influenced comprehensive changes for the 5G Toolbox process, it failed to drive policy changes to the Cyber Diplomacy Toolbox and external CCB assistance initiatives. Leveraging my discursive-institutionalist framework, I argue that the varying influence of European digital sovereignty discourse on these policy changes was conditioned by the EU's existing external action competences, reputational concerns, and (perceived) legitimacy issues. By foregrounding the integration and entanglement of cyber capacity issues with contemporary geostrategic behaviour, this study offers novel empirical and theoretical contributions to understanding 'the politics of cyber security' (Dunn Cavelty & Wenger, 2022, p. 4), especially in the EU context. Additionally, it contributes to contemporary debates on 'digital sovereignty' in cyber-IR and to more longstanding debates about the EU as a coherent actor in EU Studies. For the former body of scholarship, my contribution demonstrates how reputational concerns and institutional context can produce incoherence between the expression of digital sovereignty claims and the pursuit of sovereigntist policies in practice. Chapter 5's finding that reputational concerns conditioned EU elites' engagement with digital sovereignty discourse in some contexts suggests a potential emotional and/or ontological security dimension to geostrategic behaviour.

Building upon this article, Chapter 6 explores the EU's evolution as a geostrategic cyber actor in greater depth, with a focus upon the potential ontological security dimension to the EU's quixotic geostrategic behaviour. It asks: *how has the EU's engagement with spatial (b)ordering practices in cyberspace shaped its evolution as a strategic cyber actor, and to what extent have ontological security drives underpinned this relationship?* Drawing upon critical geopolitics and ontological security studies, this paper theorizes that actors may

engage in spatial (b)ordering practices in and through cyberspace to manage their ontological security drives, which may manifest as geostrategic behaviour.

Leveraging scores of policy documents and elite interviews, my analysis finds that EU actors have deployed various spatial (b)ordering moves, including digital sovereignty claims, to manage the Union's ontological security needs over the 2009-2024 timeframe. This reveals how cyber insecurities have become framed as existential issues in the EU (not only material security concerns), which have introduced imperatives to manage the EU's stability of being in an increasingly uncertain global environment. At the same time, the EU's new global approach has introduced tensions between its historical self-representation as an a-geopolitical actor and its contemporary geostrategic outlook, generating further ontological security management responses in policymakers, which have manifested as spatial (b)ordering moves towards cyberspace.

More broadly, by exploring the understudied 'ontological security' dimension to the EU's geostrategic turn, the article offers an alternative approach to dominant explanations in IR and EU Studies on geostrategic competition. This article uncovers an overlooked dimension to cybersecurity policymaking, providing further theoretical tools for making sense of the relationship between ontological security, sovereignty, and geopolitics in other foreign policy contexts. The research questions examined by the integrated thesis are summarized below in Table 1.2.

Research questions covered by thesis	
Primary research question: *What explains and characterizes geostrategic behaviour in and through cyberspace, and what are the implications of these dynamics for the nature of sovereignty and geopolitics in the digital age?*	
Article -Chapter	**Article research question**
1 – Chapter 4	How do powerful donors perceive capacity building assistance for digital development as shaping their strategic advantage? And which factors have shaped variation in their provision of capacity building assistance to developing states?

2 – Chapter 5	To what extent has European digital sovereignty discourse driven changes to EU cyber-external action policies?
3 – Chapter 6	How and why has the EU's engagement with spatial (b)ordering practices shaped its evolution as a global cyber actor?
Table 1.2. Research questions of the thesis.	

Summary

This thesis provides the first in-depth, multidimensional examination of geostrategic competition in and through cyberspace using a critical ontological approach as a shared point of departure. By foregrounding the integration and entanglement of cyber capacity issues with contemporary geostrategic behaviour, this integrated thesis offers novel empirical and theoretical contributions to approaching geostrategic phenomena in the digital age, particularly in the EU context.

Foremost, by examining the EU's puzzling evolution as a geostrategic actor in the context of cyberspace through a critical ontological approach, this thesis moves beyond the field's overwhelmingly state-centric approach to cyber geopolitics (Liebetrau & Christensen, 2020) and advances contemporary debates about Sino-American geostrategic competition, which have tended to revolve around questions of territory and state-based power. Instead, my thesis provides novel analytical tools, drawing upon critical geopolitics and ontological security studies, to move beyond Westphalian assumptions and/or cyber capabilities as key variables. By adopting this approach, it is possible to examine the EU as a geopolitical 'player' and uncover what practices, ideas, and tools underlie the EU's geostrategic ambitions.

Broadly, the thesis articles identify several influential factors which have characterized geostrategic behaviour in and through cyberspace, including ontological security concerns and reputational variables, which have been scarcely interrogated by mainstream scholarship. My dissertation research reveals how contemporary geostrategic

competition has been characterized by actors' efforts to build greater capacity in and through cyberspace by deploying a variety of hard (infrastructural) and soft (regulatory) tools. However, I argue that, counter to dominant accounts, geostrategic competition has not only shaped by systemic variables and material capabilities, but reputational concerns and *perceptions* about the capacity to act in that context. Such perceptions have, for example, have shaped EU, US, and Chinese engagement with capacity building assistance and the EU's sovereigntist claims in and through cyberspace. Moreover, I find in the context of EU external action that such behaviour has been mediated by EU policy actors' ontological security drives, not only material security concerns. By theorizing the relationship between a collective actor's perceptions of (cyber) capacity and ontological security drives in and through cyberspace, this study advances efforts by cyber-IR scholars to 'integrate cyberspace with broader concepts and theories of IR' from the 'periphery into the core of the [IR] discipline' (Foulon & Meibauer, 2024, p. 426).

Altogether, these findings demonstrate how contemporary geostrategic competition in the digital age is also characterized by dynamics of 'in betweenness' and adaptation—that is, a dialectical negotiation between 'space' and 'place' (Adams & Warf, 1997, p. 161). In chapters 4-6, I show how actors such as the EU have endeavoured to create 'places' out of 'cyber*space'* through processes of horizontal territorialization (that is, by expanding EU control over *virtual* cyberspace, including through sovereigntist claims) and via *vertical integration* (e.g. attaching cybersecurity instruments/technologies to adjacent issues, such as security, sovereignty, and digital development), thereby 'deepening' cyberspace by extending it across the technology stack and/or across policy areas under the purview of an actor's (legitimate) control.

By the same token, I show in Chapters 5 and 6 how the EU's geostrategic turn has been characterized by dynamics of *temporal* liminality—that is, between the EU's past and

present ‘selves’ as a global actor. Specifically, the EU’s self-narrative as a global cyber actor has sought to both reproduce and transcend its past self-image: reinforcing its past role as a global technological leader by adopting new forms of spatial ordering and control and a new ‘mindset’ to global interdependence. Presently, the EU’s geostrategic turn appears to walk a delicate, uncertain tightrope between embracing an orthodox ‘modernist’ geopolitical approach and its historical commitment as a liberal global actor. This rhetorical positioning has, in turn, encouraged the EU to distance itself from other global actors through practices of ‘geopolitical othering’. Altogether, this dissertation improves our understanding about the complex relationship between physical territoriality, the exercise of sovereign authority, and global actors’ sense of agency in ‘hybridized’ virtual/physical world.

Chapter conclusion

Cyberspace has become deeply entangled with questions of systemic change and international order, particularly geopolitical competition and discourses of weaponized interdependence (see for example Drezner et al., 2021). Yet, only two decades ago, observers such as John Perry Barlow (in this chapter’s epigraph) had characterized geopolitics and sovereigntist behaviour in cyberspace as virtually inconceivable. Rather, the ‘World Wide Web’ was expected to revolutionize classical international order and the authority of national governments. With its low entry barriers and a networked architecture which elides state boundaries, cyberspace was believed to promise a world of emancipation from state control (Zekos, 1999; Barlow, 1996).

While the honeymoon age of ‘cyber optimism’ has clearly faded, we still lack an adequate understanding of what ‘cyber geopolitics’ and ‘sovereignty’ in and through cyberspace means, including its drivers and evolving consequences for international relations. In the next chapter, I review scholarly approaches to geopolitics in and through

cyberspace. While the emerging field of ‘cyber studies’ and/or ‘cyber-IR’ has significantly flourished over the last two decades, there remain significant tensions in theory and practice. These lacunae only underline the importance of examining the drivers and characteristics of geostrategic behaviour in and through cyberspace, especially in the EU context.

Chapter 1 Reference List

Adams, P. C., & Warf, B. (1997). Introduction: Cyberspace and geographical space. *Geographical Review, 87*(2), 139–145. https://doi.org/10.1111/j.1931-0846.1997.tb00067.x.

Acemoglu, D., & Johnson, S. (2023). *Power and progress: Our thousand-year struggle over technology and prosperity.* PublicAffairs.

African Union. (2020). *The digital transformation strategy for Africa* (2020–2030).

Agnew, J. (1994). The territorial trap: The geographical assumptions of international relations theory. *Review of International Political Economy, 1*(1), 53–80. https://doi.org/10.1080/09692299408434268

Agnew, J. and Corbridge, S. (1989) The new geopolitics: The dynamics of geopolitical disorder. In R J. Johnston and P. J. Taylor (eds) *A World in Crisis?: Geographical Perspectives*. Oxford: Blackwell, 266–288.

Agnew, J. and Corbridge, S. (1995) *Mastering Space*. London: Routledge.

Arquilla, J., & Ronfeldt, D. (Eds.). (2001). *Networks and netwars: The future of terror, crime, and militancy.* RAND National Security Research Division. https://www.rand.org/pubs/monograph_reports/MR1382.html/

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security, 1(*2), 176–198. doi:10.1017/eis.2016.8.

Barkawi, T. (2016). Decolonising war. *European Journal of International Security,* 1(2), 199–214. https://doi.org/10.1017/eis.2016.7.

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*. https://www.eff.org/cyberspace-independence.

Bauerle Danzman, S., & Meunier, S. (2024). The EU's geoeconomic turn: From policy laggard to institutional innovator. *JCMS: Journal of Common Market Studies, 62*(5), 1097–1115. https://doi.org/10.1111/jcms.13599

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security, 31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887.

Berenskoetter, F. (2017). Approaches to Concept Analysis. *Millennium: Journal of International Studies, 45*(2), 151-173. https://doi.org/10.1177/0305829816651934.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue, 44*(2), 147–164. http://www.jstor.org/stable/26302224.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology.* Oxford University Press.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization, 75*(1), 39–70. doi:10.1017/S002081832000051X.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Cambridge, MA: Harvard University Press.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security, 31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885.

Carpenter, C., & Hollis, D. (2023). A victim's perspective on international law in cyberspace. *Lawfare*. Retrieved from https://www.lawfaremedia.org/article/a-victim-s-perspective-on-international-law-in-cyberspace.

Collett, R., & Barmpaliou, N. (2021). International cyber capacity building: Global trends and scenarios. *European Institute for Security Studies.* Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.

Council of the European Union. (2021, March 22). Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy. https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

Council of the European Union. (2022, May 10). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/.

Csernatoni, R. (2022). The EU's hegemonic imaginaries: From European strategic autonomy in defence to technological sovereignty. *European Security, 31*(3), 395–414. https://doi.org/10.1080/09662839.2022.2103370.

Dodds, K., 2019. *Geopolitics: A Very Short Introduction*. Oxford University Press, Oxford.

Drezner, D. W., Farrell, H., & Newman, A. L. (2021). *The uses and abuses of weaponized interdependence*. Brookings Institution Press.

Dunn Cavelty, M. (2018). Europe's cyber-power. *European Politics and Society, 19*(3), 304–320. https://doi.org/10.1080/23745118.2018.1430718.

Dunn Cavelty, M., & Wenger, A. (Eds.). (2022). *Cyber security politics: Socio-technological transformations and political fragmentation.* Routledge.

Eberle, J., & Daniel, J. (2022). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. *Political Geography, 92*, 102502. https://doi.org/10.1016/j.polgeo.2021.102502.

Eudaily, S. P., & Smith, S. (2008). Sovereign geopolitics? Uncovering the 'sovereignty paradox.' *Geopolitics,* 13(2), 309–334. https://doi.org/10.1080/14650040801991621.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2020). The EU's Cybersecurity Strategy for the Digital Decade [JOIN/2020/18final].

European Commission. (2022). Roadmap on critical technologies for security and defence. [COM(2022) 61final]. https://commission.europa.eu/system/files/2022-02/com_2022_61_1_en_act_roadmap_security_and_defence.pdf/

European Commission. (2025). The Digital Europe Programme. https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

European External Action Service. (2020, September 14). Cyber diplomacy and shifting geopolitical landscapes [Press release]. https://www.eeas.europa.eu/eeas/cyber-diplomacy-and-shifting-geopolitical-landscapes_en.

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs, 100*(6), 2379–2397. https://doi.org/10.1093/ia/iiae231.

Flockhart, T. (2020). Is this the end? Resilience, ontological security, and the crisis of the liberal international order. *Contemporary Security Policy*, 41(2), 215–240. https://doi.org/10.1080/13523260.2020.1723966.

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy, 45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

General Secretariat of the Council. (2022). A strategic compass for security and defence [7371/22]. Council of the European Union.

Giddens, A. (1985). *The nation state and violence: Volume two of A contemporary critique of historical materialism*. Polity.

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, 30(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145.

Gomez, M. A., & Whyte, C. (2021). Breaking the myth of cyber doom: Securitization and normalization of novel threats. *International Studies Quarterly, 65*(4), 1137–1150. https://doi.org/10.1093/isq/sqab034.

Guzzini, S. (2012). *The return of geopolitics in Europe?: Social mechanisms and foreign policy identity crises.* Cambridge University Press.

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: At the crossroads of politics,

sovereignty and cooperation. *Policy Design and Practice*, 6(2), 146–159. https://doi.org/10.1080/25741292.2023.2199960.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security, 38*(2), 7–40. http://www.jstor.org/stable/24480929

Kello, L. (2017). *The Virtual Weapon and International Order.* Yale University Press.

Kello, L. (2022). *Striking back: The end of peace in cyberspace—and how to restore it*. Yale University Press.

Klinke, I. (2021). On the history of a subterranean geopolitics. *Geoforum, 127*, 356–363. https://doi.org/10.1016/j.geoforum.2019.10.010.

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.

Krickel-Choi, N. C. (2022). State personhood and ontological security as a framework of existence: moving beyond identity, discovering sovereignty. *Cambridge Review of International Affairs, 37*(1), 3–21. https://doi.org/10.1080/09557571.2022.2108761.

Kuus, M. (2011). Policy and geopolitics: Bounding Europe in EUrope. *Annals of the Association of American Geographers, 101*(5), 1140–1155. https://doi.org/10.1080/00045608.2011.577362.

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review,* 22(3), 482–506. https://doi.org/10.1093/isr/viz022.

Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control.* MIT Press.

Liebetrau, T., & Christensen, K. K. (2021). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security,* 6(1), 25–43. doi:10.1017/eis.2020.10.

Lupovici, A. (2023). Ontological security, cyber technology, and states' responses. *European Journal of International Relations, 29*(1), 153-178. https://doi.org/10.1177/13540661221130958.

Madiega, T. (2020). Digital Sovereignty for Europe Digital Sovereignty: State of Play (Report no. PE 651.992). *European Parliamentary Research Service.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf .

McCarthy, D. R. (2015). *Power, information technology, and international relations theory: The power and politics of US foreign policy and the internet*. Palgrave Macmillan.

McNamara, K. R. (2023). Transforming Europe? The EU's industrial policy and geopolitical

turn. Journal of European Public Policy, 31(9), 2371–2396. https://doi.org/10.1080/13501763.2023.2230247.

Ministry of Foreign Affairs of the People's Republic of China. (2016, September 7). Position Paper of the People's Republic of China at the 71st Session of the United Nations General Assembly. Retrieved from https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367342.html/

Mitzen, J. (2018). Anxious community: EU as (in)security community. *European Security, 27(*3), 393–413. https://doi.org/10.1080/09662839.2018.1497985

Moisio, S., & Paasi, A. (2013). Beyond State-Centricity: Geopolitics of Changing State Spaces. *Geopolitics,* 18(2), 255–266. https://doi.org/10.1080/14650045.2012.738729.

Moravcsik, A. (1998). *The choice for Europe. Social purpose and state power from Messina to Maastricht.* Routledge.

Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security,* 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Nye, J.S. (2011). *The Future of Power.* New York: PublicAffairs.

Ó Tuathail, G. (1998). Postmodern geopolitics? The modern geopolitical imagination and beyond. In *Rethinking geopolitics* (1st ed., p. 23). Routledge. https://doi.org/10.4324/9780203058053.

Ó Tuathail, G., & Agnew, J. (1992). Geopolitics and discourse: Practical geopolitical reasoning in American foreign policy. *Political Geography*, 11(2), 190–204. https://doi.org/10.1016/0962-6298(92)90048-X.

Onar, N. F., & Nicolaïdis, K. (2013). The Decentring Agenda: Europe as a post-colonial power. *Cooperation and Conflict, 48*(2), 283-303. https://doi.org/10.1177/0010836713485384/.

Pawlak, P. (2016). Capacity building in cyberspace as an instrument of foreign policy. *Global Policy, 7*(1), 83–92. https://doi.org/10.1111/1758-5899.12298.

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the internet and the global digital order. *Policy & Internet*, 14(1), 13–27. https://doi.org/10.1002/poi3.296.

Richmond, N. (2019, March 4). Operation Cloud Hopper Case Study. *Software Engineering Institute, Carnegie Mellon University*. https://insights.sei.cmu.edu/blog/operation-cloud-hopper-case-study/.

Sjursen, H. (2011). Not so intergovernmental after all? On democracy and integration in European Foreign and Security Policy. *Journal of European Public Policy,* 18(8), 1078–1095. https://doi.org/10.1080/13501763.2011.615194.

Slayton, R. (2016). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. *International Security*, 41(3), 72–109. https://www.jstor.org/stable/26777791.

Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy,* 35(3), 468–486. https://doi.org/10.1080/13523260.2014.959261.

Smeets, M. (2022). *No shortcuts: Why states struggle to develop a military cyber-force.* Hurst Publishers.

Stevens, T. (2015). *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.

Stevens, T. (2023). *What is cybersecurity for? Bristol University Press*.

Subotić, J. (2016). Narrative, ontological security, and foreign policy change. *Foreign Policy Analysis,* 12(4), 610–627. https://doi.org/10.1111/fpa.12089.

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy,* 45(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739.

Taddeo, M. (2017). Cyber conflicts and political power in information societies. *Minds and Machines, 27*(2), 265–268. https://doi.org/10.1007/s11023-017-9436-3.

Tan, Y., Dallas, M., Farrell, H., & Newman, A. (2025). Driven to self-reliance: Technological interdependence and the Chinese innovation ecosystem. *International Studies Quarterly,* 69(2), 1-16. https://doi.org/10.1093/isq/sqaf017.

Thomson, J. (1995). State sovereignty in international relations: Bridging the gap between theory and empirical research. *International Studies Quarterly, 39*(2), 213–233. https://doi.org/10.2307/2600847.

US Department of State. (2024). United States International Cyberspace & Digital Policy Strategy. https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

Von der Leyen, U. (2024, February 28). Speech by President von der Leyen at the European Parliament Plenary on strengthening European defence in a volatile geopolitical landscape. *European Commission*. https://enlargement.ec.europa.eu/news/speech-president-von-der-leyen-european-parliament-plenary-strengthening-european-defence-volatile-2024-02-28_en

Weber, V. (2020). Making sense of technological spheres of influence. London: *LSE IDEAS.* https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Technological-Spheres-of-Influence.pdf.

Zekos, G. (1999). Internet or electronic technology: A threat to state sovereignty. The

Journal of Information, Law and Technology, 1999(3). http://elj.warwick.ac.uk/jilt/99-3/zekos.html.

Zielonka, J. (2006). *Europe as empire: The nature of the enlarged European Union*. Oxford University Press.

Chapter 2: Geostrategic behaviour in the 'digital age' in international relations scholarship

Chapter overview

This chapter covers the key themes, tensions, and questions which comprise the dissertation's research agenda. After defining key concepts, this chapter explores how cyberspace has challenged classical IR assumptions about the relationship between geography and strategic advantage, drawing upon the IPE, critical, and digital politics literatures. Additionally, I consider the insights of critical security and constructivist scholarship about the rise of sovereigntist and geopolitical discourses and practices. In undertaking this exercise, this chapter also aims to offer a distinct contribution to the cyber-IR field; to the author's best knowledge, this review constitutes the first attempt to synthesize various scholarly approaches to geopolitics and sovereignty *in and through* cyberspace into one collective body of work.[3]

Throughout this chapter, I adopt a critical ontological approach to explore how the concepts of 'cyberspace', 'geopolitics', and 'sovereignty' function as both academic 'categories of analysis' and real-life 'categories of practice' (Berenskoetter, 2017). [4] Ontology refers to the assumptions or claims one makes about *being,* about 'what *is* […], what e*xists*,' and about 'the constituent units of reality,' (Hay, 2011, p. 463). This approach serves as a valuable basis for interrogating the constitutive language and 'grammar' of cyber-

[3] As Foulon and Meibauer (2024) demonstrate, cyber-IR scholarship has often approached cyberspace either through a domain perspective ('within cyberspace') *or* a systemic approach ('through cyberspace). While there have been concerted efforts to consider both dimensions of cyberspace in approaches to geostrategic competition (e.g. Fischerkeller & Harknett, 2019; Foulon & Meibauer, 2024), a comprehensive *review* of how scholars have approached geostrategic competition at both levels of analysis—one which treats these accounts as a collective body of work—is absent in cyber-IR.

[4]Whereby 'categories of analysis' are understood to be foundational to the construction of academic theories and/or serve as tools for analytical reasoning and/or heuristic devices, and 'categories of practice' refer to the way in which the concept is socially constructed in real life and/or 'lived' in experience (Berenskoetter, 2017, p. 155). Importantly, as I note further in this chapter, these two categories are not hermetically sealed; rather, they are often intertwined in practice, given that scholars are 'part of the world they are studying', in line with interpretivist approaches to research (see also Cristiano et al., 2023).

geopolitics and sovereignty, enabling us to identify how both scholarship and policy practices have co-shaped the production of knowledge on cyber-geopolitics.

Through this lens, I review how extant scholarship, notwithstanding its pathbreaking contributions to the IR discipline, has left important gaps in our understanding about the nature and drivers of geostrategic behaviour in and through cyberspace—especially with regards to the European Union context. Altogether, mainstream cyber-IR scholarship has debated the nature of power relations and territorial consequences of geopolitics in and through cyberspace, largely through a state-centric, materialist perspective. Within this interdisciplinary corpus of work, there are significant areas of disagreement and conceptual opacity regarding the basic features and aims of geostrategic competition in the digital age. Consequently, we have yet to fully understand the co-constitutive relationship between sovereigntist claims, geopolitical competition, and the sociotechnical nature of cyberspace.

To advance our understanding, I consider how critical IR literature, such as critical geopolitics, ontological security studies, and constructivist approaches, could offer valuable tools for making sense of these dynamics. While offering several promising points of departure, extant scholarship has not adequately explored the nexus between geostrategic behaviour and cyberspace, especially in the context of non-traditional strategic actors, such as the EU. Altogether, these themes and issues coalesce into three core areas analytical inquiry and critique addressed by the dissertation's three research articles.

To offer essential background for the reader, the below section first positions my approach to 'cyber' concepts within the extant scholarship and provides a brief background of the 'rise' of geopolitics in and through cyberspace.

2.1. Ontologies about the nature and scope of 'cyberspace'

I understand cyberspace as 'a complex socio-technical system' with fluid boundaries, whereby technologies and politics are considered inseparable from each other (Dunn Cavelty & Wenger, 2022). My approach coheres with an 'inclusive' approach to cyberspace, which incorporates both infrastructural and ideational dimensions to the definition (Betz & Stevens, 2011; see also Foulon & Meibauer, 2024, p. 439).

As I explore below, a critical ontological approach to cyberspace unmasks several productive struggles to generate knowledge about cyberspace. First, at the level of academic scholarship, scholars examining cyberspace from an IR perspective have advanced varying ontological approaches to the basic nature of cyberspace, demonstrating its challenges to classical understanding of global politics.[5] Meanwhile, policymakers across the world have struggled to conceptualize and define cyberspace. Accordingly, this approach emphasizes that academic knowledge production about the 'nature' of cyberspace and its consequences for international politics is not wholly divorced from practical knowledge, not least because of the technical complexities inherent to cybersecurity politics (Cristiano et al., 2023).[6]

Underlying the baseline scholarly consensus that cyberspace is a complex, multi-layered environment lies disagreement about the domain's fundamental features, such as the number, substance and type of 'layers' of cyberspace and whether to include infrastructure in its definition (see for example Kello, 2013, p. 17; Choucri & Clark, 2012; Betz & Stevens, 2011; in Table 2.3). However, more recently, cyberspace is commonly understood to be

[5] Through a similar perspective, it can be understood how IR theories themselves can be understood as adhering to distinct '*scientific ontologies'*—that is, a 'catalog—or map—of the basic substances and processes that constitute world politics', including the core units of analysis (e.g. states), and the basic determinants of 'power' and 'security' (Lerner & O'Loughin, 2023, p. 3, quoting Jackson and Nexon 2013, 550.)

[6] This is not confined to cyber-IR, but rather a wider phenomenon of political science research. For a wider discussion and case analysis relevant to IR theory and practice, see Lerner & O'Loughlin 2023, Berenskoetter, 2017; Guzzini, 2013. Notably, Guzzini (2013) explored how classical realists developed knowledge about 'the balance of power' from both a 'sense of history and the experience of politics' (p. 528).

jointly constituted by a 'social space' and a material 'infrastructural' layer (Lambach, 2020, p. 484).

Networked layers of cyberspace	**Description**	**Characteristics**
Hard infrastructural layer	Hardware components which form the architecture of cyberspace – ICT/ telecommunications infrastructure (e.g. TV towers), computers, submarine cables, etc.	▪ Material / physical
Technical / informational layer	Software – social media, domain names, IP protocols, social media, search engines, containing *information*	▪ Informational: primarily virtual, with material elements
Human layer	Human participants– be they customers/consumers, corporate actors, government officials, computer users	▪ Social (physical and virtual) ▪ Individual/ ideational (immaterial)

Table 2.3. Author's conception of networked layers of cyberspace, synthesized from literature.

Notably, there is no universal agreement in scholarship about the distinguishing characteristics of cyberspace versus the digital domain—*within and across* sub-disciplines that comprise 'cyber-IR' and/or 'cybersecurity studies' (Dunn Cavelty, 2023). On the one hand, strategic studies scholarship has tended to focus upon 'cyberspace' as opposed to the 'digital domain', which could be due to the reality that 'states and international organizations have widely recognized cyberspace to be the 'fifth operational domain,' (see for example NATO, 2024; Lindsay, 2015; Maurer & Morgus, 2014). Other related scholarship, including development studies and international political economy, has concentrated upon 'the digital domain' *and* cyberspace somewhat interchangeably (for a broad review, see Dunn Cavelty & Wenger, 2020). Thus, despite conceptual fuzziness, there is considerable overlap between these literatures in terms of the themes, policy issues, and case studies covered in their work.

As Betz and Stevens have observed, ‘Where you find cyberspace and what it looks like depend a lot on the reason you are looking for it in the first place,’ (2017, p. 106).

Policy conceptualizations

The conceptual fluidity surrounding ‘cyber’ issues have also borne out in the policymaking context, whereby ‘cyberspace’ and ‘the digital domain’ remain slippery and contested concepts (Dunn Cavelty & Egloff, 2019). Examining official digital and cyber strategies reveals a diversity of conceptions about cyberspace and the digital domain, demonstrating that they are often considered transversal political and strategic environments (Betz & Stevens, 2011; Pawlak, 2018; Branch, 2021). For example, while Russia has conceived of cyberspace as a facet of ‘information security’ rather than a distinct domain of its own, China has adopted a distinct view of cyberspace, as evidenced by its efforts to secure ‘cyber sovereignty’ and achieve a ‘community of common destiny in cyberspace,’ (Broeders et al., 2019; Creemers, 2024). Notably, the practical definitions of these concepts have shifted over time and in line with different policy areas (Barrinha & Christou, 2022; Betz & Stevens, 2011). As Dunn Cavelty and Egloff observed, ‘cyber security is moving upward in the political agenda and expanding sideways as a problem area to a multitude of additional policy domains with advancing digitalization,’ (quoted in Dunn Cavelty & Wenger, 2022, p. 2).

For Western policymakers, ‘cyber’ has recently come to be seen as an enabler for activities in the digital domain, as seen with debates on the importance of ‘cybersecurity’ for digital sovereignty (Bellanova et al., 2022). The United Kingdom’s *National Cyber Strategy* outlined how cyber resilience is a key pillar of ‘building a resilient prosperous digital UK’ (2022, p. 6); and its *Digital Strategy* (2022) stressed how internet access and cybersecurity capabilities are seen as ‘critical building blocks of the digital economy’; whereby ‘cyber

power' alongside digital infrastructure seen as a measure of strength for its global position. Similarly, the United States' development agency, USAID, stressed in 2021 that cybersecurity 'must become a first-order strategic and operational priority' for its digital development projects: indeed, it 'should be thought of as a core thread that runs through all aspects of USAID's technology programs in order to ensure digital sustainability and resiliency,' (2021).

Across the channel, official EU documents now link 'cyber' to 'network and information security' as an *enabler* of the 'digital' and as a 'fifth domain of warfare,' (Council of the European Union, 2015; Pawlak, 2018, p. 20). By contrast, 'the digital domain' has come to be understood by EU bodies as a more encompassing socio-technical space, including the internet, digital technologies, 'space', the 'Digital Market', data, and an 'EU digital identity' (European Commission, 2021). Presently, Brussels understands cybersecurity as a key strategic 'priority', 'pillar', and/or 'cornerstone' for achieving European digital sovereignty (Bellanova et al., 2022; General Secretariat of the Council, 2022; European Commission, 2022). The EU's Commission President, Ursula von der Leyen, explained in 2019 that 'cyber security and digitalisation are two sides of the same coin' (European Commission, 2019). Thus, Brussels' current approach towards the global digital domain relies upon cybersecurity as a key foundation and priority area, alongside AI and supercomputing (General Secretariat of the Council, 2022). The EU's official approach to cyberspace aligns closely with that of Rebecca Slayton, which she defines as the 'infrastructure that *enables* digital electronic computing and communications,' whereby the 'infrastructure is physical, even though its purpose is informational,' (Slayton, 2017, p. 74, emphasis added by author). [7]

[7] I expound upon this overlap in Chapter 5.

Finally, defining 'cyber' concepts and is complicated by the reality that the meaning of many basic concepts in IR scholarship, often used in concatenation with 'cyber'—such as power and security—are themselves contested (Berenskoetter, 2017). Notably, the concept of 'security' has a variety of different fundamental meanings to different communities and is shaped by the sociopolitical context (Dunn Cavelty & Wenger, 2022). Hansen and Nissenbaum show how, by responding to the Estonian 2007 cyberattacks, the concept of 'cybersecurity' met the threshold of 'securitization' as its 'grammar' was premised upon the concept's associations with the 'collective reference objects of the "state", "society", "the nation" and "the economy,"' (2009, p. 1155). As these collective associations were absent in earlier notions of 'computer security' and 'network security', they had previously escaped the definition of 'securitization' as laid out by the Copenhagen School (Hansen & Nissenbaum 2009, p. 1155). Therefore, the particular *securitization moves* undertaken by policymakers around the construction of 'cybersecurity' threats laid the basis for cybersecurity's inception into the Copenhagen School branch of security studies.[8]

Over the past decade, cybersecurity threat discourse has typically linked 'technical systems to more traditional threat politics,' including national security issues (Dunn Cavelty & Wenger, 2022, p. 3). Yet, due to the transnational, sociotechnical nature of cyberspace, scholars have deemed state-centric studies inadequate for fully capturing the multifaceted reality of cybersecurity practices (Liebetrau & Christensen, 2021; see also Sukumar et al., 2024). As Liebetrau and Christensen contend, 'much of the politics of cyber security play

[8] For notable works, see Lene Hansen and Helen Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, *International Studies Quarterly*, 53(4), 1155–1175 (2009). https://doi.org/10.1111/j.1468-2478.2009.00572.x; Thierry Balzacq, Sarah Léonard, and Jan Ruzicka (2015). 'Securitization' revisited: Theory and cases, *International Relations*, 30(4), 494–531. https://doi.org/10.1177/0047117815596590; George Christou (2016), *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Palgrave Macmillan; Barry Buzan, Ole Wæver, and Jaap de Wilde (1998), *Security: A new framework for analysis*, Lynne Rienner Publishers.

out among actors and in sites and spaces of security politics that evade traditional forms of national security' due to the interconnected, diffuse, and ever-evolving nature of digital technologies (2021, p. 6).

More pertinent to this thesis, traditional state-centric approaches to classical 'national security issues' in and through cyberspace are complicated by the emergence of geostrategic and sovereigntist concepts, including at the level of EU supranational discourse. This is briefly discussed in the next section, which provides background to the puzzle examined by this thesis.

2.1.2. Background to cyber studies: From cyber utopia, to cyber war, to subthreshold competition in cyber-IR

Studying geostrategic behaviour in and through cyberspace has been approached by a recent wave of cyber-IR literature emphasizing the significance of cyberspace as situated *within and through* the wider global environment and vis-à-vis other facets of strategic and foreign policy (see for example Buchanan, 2020; Dunn Cavelty & Wenger, 2022; Foulon & Meibauer, 2024). To varying extents, these debates adapt and/or flow from earlier arguments in the cyber-IR literature about the nature of power in and through cyberspace. These are briefly sketched out below.

In the late 1990s, notions of 'digital sovereignty' and 'cyber-geopolitics' were virtually inconceivable in popular imagination, as emblematized by Barlow's (in)famous 'Declaration of the Independence of Cyberspace' (Barlow, 1996; cf. Arquilla & Ronfeldt, 1993). Cyberspace had promised to revolutionize the future of democracy, obliterate territorial borders, and undermine the sovereign authority of traditional state actors (Barlow, 1999; see also Dodds, 2019, p. 4). With its low entry barriers, public internet backbone, and

fluid, networked architecture, cyberspace heralded collective emancipation from state control (Barlow, 1999). As Seidl eloquently observed,

> in the last decades of the twentieth century, digitalisation became strangely untethered from its military and scientific origins and the uneven geography of its material underpinnings. It was as if the world had forgotten that the internet had 'a body of glass, copper, silicon, and a thousand other things' (Tarnoff 2022, x); a body which stretches across ocean floors and weaves through continents, often following earlier telegraph networks and railway routes and thus reflecting the colonial topography of global infrastructure (2024, p. 2034).

However, utopic visions of cyberspace as an emancipatory, borderless society were shattered by a flurry of destructive and disruptive cyber-enabled events in the noughties and 2010s,[9] which demonstrated states' resolve to ensure control and security in and through cyberspace, and the rising position of 'cyber' issues in national security contexts (Nye, 2014; Hansen & Nissenbaum, 2009). Thus, cyberspace has been characterized by IR scholarship as an emerging domain for conflict (Harknett et al., 2022; Kello, 2022); subversion (Maschmeyer, 2022); exploitation, and intelligence contests (Chesney & Smeets, 2023). In Eastern Europe, for example, scholars argued that cyber operations in various forms—from influence operations to attacks on critical infrastructure—have been an enduring facet of Russian foreign policy (Kello, 2017). As the American and Israeli joint operation 'Stuxnet' demonstrated, cyberattacks and espionage have long featured in the playbooks of strategic rivals (see for example Ajili & Rouhi, 2019; Lupovici, 2022; Buchanan, 2020).

Against this backdrop, an earlier wave of cyber-IR literature revolved around the question of 'cyber war', cyber escalation dynamics, and their potential to revolutionize the nature of interstate conflict (Arquilla & Ronfeldt, 1993; Kello, 2013; Rid, 2013). Currently, consensus holds that cyber activities (broadly conceived) generate strategic and operational

[9] Examples include the 2007 Estonian cyberattacks, 2011 Stuxnet, 2017 WannaCry and NotPetya. For a brief review of the 2007 cyberattacks and their impact on cyber strategies, see for example Kello (2022, pp. 126-128).

uncertainties for states, leading to significant policy challenges (Kaminska, 2021; Gomez & Whyte, 2021; Kello, 2022; Dunn Cavelty & Wenger, 2022; Moore, 2022). Yet, both the strategic impact of cyberattacks, their effects on war outcomes, and the extent which states' cyber strategies fulfil wider 'grand strategies' have been heavily debated (see for example Weber, 2018; Lupovici, 2022; Falkner et al., 2024; Lonergan & Lonergan, 2023). Similarly, efforts to understand the dynamics of cyber conflict below the threshold of conventional war have given rise to controversial concepts, such as 'persistent engagement' and 'cyber deterrence', which have imbricated with real strategic doctrine (Fischerkeller & Harknett, 2019; Kello, 2022).

More recently—and more relevant to this study—cyber-IR scholarship has begun to investigate the convergence between cyberspace, (state) sovereignty, and issues of (techno)geopolitical competition (see for instance Kello, 2022; Buchanan, 2020; Broeders, 2022). Studies have responded to earlier calls in the literature to progress the debate beyond all-out 'cyberwar' towards theorizing cyber activities as shaping strategic advantage *below* the threshold of armed conflict (Harknett & Smeets, 2020; Buchanan, 2020; Maschmeyer, 2022). In this emerging work, cyberspace has been framed as a new domain of strategic competition and (in)stability within the context of wider systemic dynamics (Kello, 2022; Foulon & Meibauer, 2024; Buchanan, 2020; see also Kostyuk & Gartzke, 2022).

On the one hand, these debates have revived older arguments about the 'revolutionary' nature of cyberspace: in Kello's words, 'Vital security interests and the nation's political integrity could be affected by forms of conflict less than war. The nature of interstate rivalry has changed,' (2022, p. 127). On the other hand, this nascent 'integrative' turn in scholarship has responded to changing empirical realities about the perceived significance of cyberspace for global competition by a variety of cyber actors. For example, the current trend towards the 'Balkanization of the internet', cyber- 'spheres of influence',

and states' claims of 'cyber sovereignty' evidences the rise of geostrategic behaviour in and through cyberspace in strategic doctrines and foreign policy discourses (Lewis, 2020; Chander & Sun, 2021).

As I elaborate below, this study can also be situated within a wider discipline of studies on geopolitics and sovereignty, thereby straddling several subfields in IR literature. This literature has made great strides towards improving our understanding about the global rise of geostrategic behaviour in and through cyberspace. However, there remain significant gaps, omissions, and tensions in extant scholarship which point to the urgent need for greater theoretical and empirical innovations on this topic. To do so, I first return to the 'basic qualities' of geopolitics and sovereignty as an initial step.

Conceptualizing 'sovereignty' and 'geopolitics' as geostrategies

As I will demonstrate in this chapter, 'sovereignty' and 'geopolitics' have a shared conceptual emphasis on *influence over a particular space and/or territory*. Both sovereignty and geopolitics can be understood as spatial ordering concepts—that is, *geostrategic concepts*. *Sovereignty* refers to the claim for either, or both, *territorial* control ('territorial sovereignty') and *functional* control over space/virtual communities (Newman, 1998). Sovereignty assertions have both internal and external dimensions. Classically, sovereignty has been defined as the internal legitimate control over and *within* one's borders in a given political space and the external principles of mutual recognition and non-interference on the basis of sovereign status (Keene, 2014; Thompson, 1995).

Geopolitics is broadly defined as 'representations of space and the spatial practices underpinning world politics' (Ó Tuathail, 1998, p. 17); a form of statecraft which is premised upon the political, social, and economic relationship between space, power, and strategy (Agnew & Corbridge, 1989; see also Dodds, 2019). This may include competition over

space through expansionist territorial goals (Guzzini, 2012) on the basis of 'grand international visions' (Kuus, 2011, p. 1141).

Alike geopolitical concepts, conceptualizations of sovereignty have both territorial and technological foundations in IR scholarship (Eudaily & Smith, 2008; see also McCarthy, 2015; p. 3; Falkner et al., 2024). In the following section, I review how popular modernist geopolitics has conceived of nation states as 'the modern summation of sovereign power' and the primary actors in geopolitical competition (Eudaily & Smith, 2008, p. 319). Yet, cyberspace disrupts the 'state-force-territory' relation in global politics which has underpinned the basis of orthodox sovereigntist and geopolitical concepts (Barkawi, 2016, p. 207).

2.2. 'Cyber-geopolitics' in mainstream IR theory: Characteristics, competition and capabilities in and through cyberspace

This section reviews how mainstream scholarship has characterized geostrategic competition *within* and *through* cyberspace, identifying shared spatial logics, tensions, and ambiguities. I demonstrate how the bulk of scholarship has adopted networked ontologies to approach geostrategic behaviour *within* cyberspace (i.e. at the 'domain' level). Strikingly, these approaches have reproduced the basic logics of two competing 'modernist' and 'postmodernist' geopolitical imaginaries of cyberspace. By contrast, geostrategic competition *through* cyberspace (i.e. the systemic level) has been predominantly approached by mainstream scholarship through the prism of realism, an IR paradigm historically linked with modernist geopolitical thought. Generally, both approaches to geostrategic competition in and through cyberspace have emphasized the significance of sovereign *interstate* behaviour, network positioning, and the possession and exercise of *cyber capabilities* as driving dynamics of competition.

Modernist geopolitical thought and its relevance to IR

Prior to elaborating domain and systemic-level accounts of geostrategic competition in and through cyberspace, it is cogent to explain what is meant by 'modernist' geopolitical thought. Popular notions of 'geopolitics' are often associated with 'modernist' or 'classical' geopolitical thought of the 19th and 20th centuries (Dodds & Woon, 2018; Deudney, 2020). The 'modern geopolitical imagination' has its roots in European statecraft, whereby a state's 'interests' was pursued through strategies which accounted for 'global conditions' which emerged from 'the European encounter with the rest of the world,' (Agnew, 2004, p. 5). Thus, geospatial analogies have a long history in constituting European statehood and European 'civilizational' logics, including early European conceptions of sovereignty in international law (Anghie, 2005). In fact, the term 'geopolitics' was coined in the 1890s by Rudolf Kjellén (Dodds & Woon, 2018), but earlier geopolitical thought on the 'shaping effects' of geographic factors are traceable to Aristotle and Montesquieu (Deudney, 2020).

Modernist geopolitical thought emphasizes the significance of material factors for strategic decision making—particularly, the interaction between political strategy, geographic variables, and changes to technology (Deudney, 2020; Gray & Roan, 1999). As Gray and Roan observe, this approach reflects the belief 'that political predominance is a question not just of having power in the sense of human or material resources, but also of the geographical context within which that power is exercised' (1999, p. 2). For classical theorists such as Alfred Mahan and Halford Mackinder,

> 'geography can be described as the mother of strategy, in that the geographical configuration of land and sea, with respect to a state's strategic policy, or an alliance between states, can exercise a twofold strategic conditioning influence: on locations important for defence, and on the routes and geographical configurations which favour an attacking

force, be it on land or sea,' (Gray & Roan, 1999, p. 3; see also Deudney, 2020, p. 279).

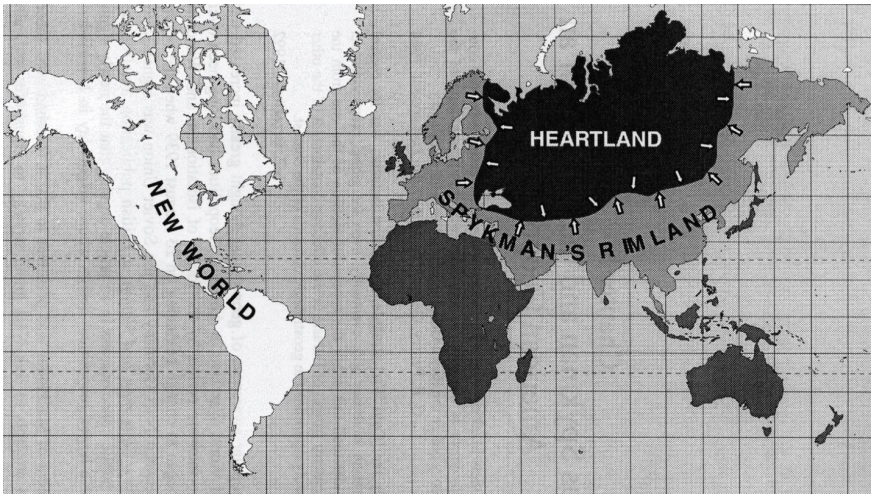


Figure 2.1. National Macedonian Academy of Sciences and Arts (MANU) with Shared Knowledge, CC BY-SA 4.0, https://creativecommons.org/licenses/by-sa/4.0, via Wikimedia Commons, as 'Heartland and Rimland'.

Modernist geopolitical approaches adhere to state-centric, Westphalian approaches to territoriality, which conceive of politics as 'territorially defined, fixed, and mutually exclusive enclaves of legitimate dominion,' (Ruggie, 1993, p. 151). Accordingly, many modernist theories of geopolitics often linked to the realist paradigm in IR scholarship (Deudney, 2020; McCarthy, 2015). Realists subscribe to notions of 'power-politics', in which the state is a unitary, rational actor making decisions in an anarchical international environment (Morgenthau, 1948). 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 (Howorth & Menon, 2009; Waltz, 1979).[10] As Zakaria writes, a 'classical' hypothesis of realist theories holds that

[10] More specifically, structural or *neorealist* subvariants of realism (Waltz, 1979; Mearsheimer, 2001), emphasize the importance of the balance of power (as the relative distribution of capabilities) between states under conditions of international anarchy. Modifying this purely structural account, *neoclassical realism* emphasizes the importance of domestic level variables as intervening variables, including the (mis)perceptions of strategic decisionmakers (e.g. Ripsman et al., 2016), between 'systemic incentives and state behaviour' (Foulon & Meibauer, 2020, p. 1209).

states 'expand their political interests abroad when their relative power increases… but only when the benefits exceed the costs' (1998, pp. 19-20).

Notably, the popularity of modernist geopolitical approaches in academic and policy discourse have waxed and waned.[11] As Chapter 1 outlined, the contemporary era has seen a revival of 'geopolitical thought.' Yet, the resurgence of 'geopolitics' as a term does not necessarily imply that contemporary 'geopolitics' conforms to modernist conceptions of the term (Agnew, 2004), despite the nationalistic appeal of modernist geopolitical imaginaries (Guzzini, 2017). Indeed, as I will explore further in this chapter, 'geopolitics' may convey a variety of meanings and/or assumptions about power and space (Deudney, 2020; Agnew, 2004), which remain underexamined by cyber-IR scholarship.

2.2.1. Domain level: Geostrategic competition within cyberspace

At the domain level, cyberspace challenges the notion that 'the grammar of strategy literally and inalienably is dictated by the distinctive requirements of *physical geography*,' (emphasis my own; Gray & Roan, 1999, p. 6). Rather than serving as the 'durable and influential template for international politics' (Dodds & Woo, 2018, p. 2; see also Spykman, 1969), scholars have argued that cyberspace has a 'fluid geography', comprised of a hybrid mix of 'physical/virtual' space and a variety of actors with varying relationships to the state (Egloff, 2019). Thus, cyber-IR scholars have widely recognized that the environmental and

[11] While modernist geopolitics approaches rose to prominence during the two World Wars, geopolitical concepts were later eschewed in Anglo-American policy circles, in part due to its association with Nazism (although key global actors, such as the United States, did not stop thinking in geopolitical terms or aims; see Dodds & Woo, 2018). Classical approaches to geopolitics later saw a resurgence during the Cold War, whereby the famous 'heartland' thesis advanced by Halford Mackinder inspired further adaptations, including by scholars such as Nicholas Spykman (see Figure 2.1). Indeed, modernist geopolitics was used as a 'method of analysis' by American scholar and foreign policymaker Henry Kissinger to rebuke liberal idealist policies and as a means to represent 'global equilibrium' and the balance of power (1979, p. 914; see also Zakaria, 1998, for a wider discussion). With the rise of globalization, the spread of the 'American liberal order', and transnationalism in the 2000s, modernist geopolitical thought declined in prominence in Western and European policy circles (Agnew, 2004), until its resurgence in the 2010s.

spatial features of cyberspace are inherently disruptive to such 'Westphalian' territorial conceptions of geography (e.g. Kello, 2013; Betz & Stevens, 2013).

As Arquilla and Ronfeldt stated, 'Cyberwar depends less on the geographic terrain than on the nature of the electronic "cyberspace," which should be open to domination through advanced technology applications,' (1993, p. 44). Due to these characteristics, cyberspace tends to 'represent a threat to the spatialized forms of intelligibility and control', as emblematized by modernist geopolitical thought (Balzacq & Dunn Cavelty, 2016, p. 186; see also Mueller 2020, p. 1).

These observations have given rise to networked ontologies of cyberspace, which 'focus on the centrality and connectivity of nodes, on externalities within the network, and on relations and flows between nodes,' and they tend to emphasize the horizontal or 'flat' dimensions of an environment (Lambach, 2020, p. 485). At first blush, all networked accounts appear diametrically opposed to modernist characterizations of geostrategic competition, as they challenge the physical /geographic assumptions of modernist geopolitics by emphasizing the decentralized, 'borderless' and transnational character of cyberspace (Lambach, 2020) and the domain's potential to depress and/or reconfigure traditional territorial (dis)advantages in conventional warfighting doctrine. However, as I discuss below, some prominent 'net-centric' accounts do not dispute the fundamental premise of classical geopolitics: that environmental (geo)spatial variables and material factors *matter* for strategic decision-making and interstate competition (Deudney, 2020; see also Gray & Roan, 2011). In contrast, other accounts adopt more critical geopolitical and constructivist assumptions and embrace 'postmodernist' geopolitical imaginaries.

Notably, networked ontologies in cyber-IR have co-evolved with the rise of 'net centric' conceptions about cyber conflict and competition in Anglo-American national security contexts. Illustrating this conception, the US Joint Chiefs of Staff described the internet in

2018 as enabling 'force projection *without the need to establish a physical presence in foreign territory*' (p. 46). Further note, for example, the distinctive emphasis placed upon as 'moving information, not people' (see Figure 2.2) in net-centric approaches, as opposed to modernist conceptions of geopolitics as moving military personnel (including tanks/ships/naval vessels/transportation vehicles) across geographic space.

Thus, networked thinking has shaped the practice of cybersecurity for several decades. At a more extreme end of the spectrum, early national security discourses, particularly in Europe and North America, perceived cybersecurity threats 'as operating at one spatial plane, that of a network' which must be controlled in order to 'protect the mobility of data' and 'the stability of networks (Balzacq & Dunn Cavelty, 2016, p. 177). Similarly, scholars such as Arquilla and Ronfeldt argued that 'future conflicts will be fought more by "networks" than by "hierarchies," and that whoever masters the network form will gain major advantages, (1993, p. 45; see Figure 2.2 and 2.3 below). Such arguments are reflective of an 'ontological predisposition toward the horizontal and the emergent, rather than the hierarchical and structured' (Lambach, 2020, p. 485).

Figure 8-17. Split-Based Operations

Figure 2.2. "Network Centric Warfare", Network Centric Warfare Department of Defense Report to Congress (2001).

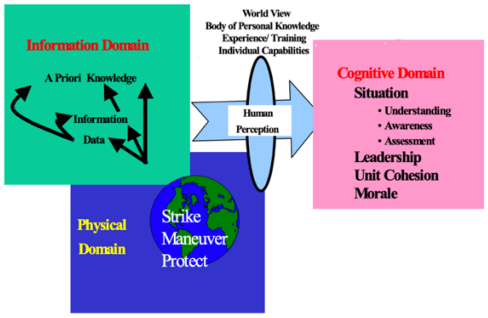
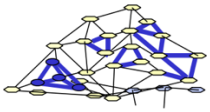
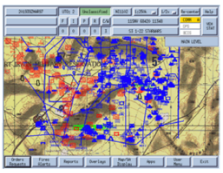


Figure 3-2. Domains of Warfare



Network -
Physical Domain



Common Operational Picture -
Information Domain

Figure 3-4. Relationship Between Physical Domain and Information Domain

Figure 2.3. US Department of Defence Representations of "Network Centric Warfare". From the US Department of Defense Report to Congress (2001, pp. 44, 51).

Earlier perspectives on net-centric warfare have been tempered by recent scholarship and adaptations to strategic doctrine (e.g. United States Joint Chiefs of Staff, 2018), although this work has still emphasized the networked structural features of cyberspace. For example, Harknett and Smeets acknowledged that 'the internet is still constrained by infrastructure,'—although 'user demand and government restrictions […] create a *"differentiated centrality",*' (2020, p. 544). They elaborate, 'unlike conventional forms of hard power, the use of cyber means is hardly mediated by geographical distance,' and 'cyberspace's interconnectedness *changes* the ability of actors to exert influence beyond their own boundaries through the use of capabilities,' (emphasis added by author, p. 544). By this account, physical geography is partly overcome by a networked logic of power which emphasizes fragmentation, fluidity, rapid access, and interconnectivity.[12]

The above domain-level approaches have emphasized the relationship between the environmental features of (cyber)space as a (new) template for military doctrine, together with material capabilities and network positioning (e.g. Arquilla & Ronfeldt, 1993). For example, networked assumptions of spatiality underlie 'cyber persistence' theory, which

[12] They distinguish cyber operations from what Kenneth Boulding termed the 'loss-of-strength gradient' (LSG) in conventional power projection, or 'the ability of an actor to deploy military force decreases with geographical distance,' (1962, pp. 79, 230–231).

conceives of actors in ‘constant contact’ due to the networked, interconnected structure of cyberspace (Harknett & Smeets, 2020). Thus, proponents of this theory contend that powerful actors such as the United States should undertake ‘persistent engagement’ to create friction and deter adversaries from achieving ‘cumulative gains’ which could shift the balance of power (Harknett & Smeets, 2020; Fischerkeller & Harknett, 2019). Some scholars have pushed back against these materialist assumptions on the basis that, ‘In practice […] interconnectedness and constant contact are not given structural conditions, but actor-specific variables,’ (Maschmeyer, 2023, p. 574).[13]

On the other hand, ‘critical’ networked ontologies may be associated with ‘postmodernist’ visions of geopolitics, which, following Ó Tuathail, emphasize ‘flows, webs, connectivity, and networks’ (p. 25) and ‘the disintegration of the Euclidian world of discrete nation-states imagined by so many political realists’ (p. 29). By emphasizing the geographic fluidity and complexity of cyberspace, ‘postmodernist’ networked approaches argue that exercising power in and through cyberspace does not simply map onto existing topographical approaches (e.g. Latour, 1996).

In particular, Actor Network Theory (ANT) approaches have placed further emphasis on both actors and objects as co-constituting (cyber)space, thereby stressing the multidimensional nature of actors and networks in this context (Balzacq & Dunn Cavelty, 2016, pp. 183-184; Latour, 1996). More provocative schemas, as advanced by Luke (1995), emphasize the new spatial configurations produced by ‘cybernetic systems’, a ‘third nature’ of space which *erodes* ‘modernist’ industrial infrastructures and modernist complexes of state building centred around ‘traditional divisions between the local, national, and global’ [thereby] creating a scalar dynamic of “neo-world orders” composed of rearranged glocal

[13]As Maschmeyer points out, Stuxnet was not reliant upon American and Israeli persistent contact with Iran’s computer systems, but damaging the regime’s nuclear enrichment centrifuges through a USB stick.

space' (Luke 1995, in O Tuathail, 1998, p. 26). In this way, 'postmodernist' geopolitical conceptions of cyberspace have tended to emphasize the 'unique' features of cyberspace and the significance of virtual realities, communities, and connections above classical geographic boundaries and interstate relations (Lambach, 2020).

Collectively, networked approaches challenge the geographic assumptions of modernist geopolitical accounts to varying degrees, stoking further debates about the relationship between physical space and geostrategic behaviour in and through cyberspace.[14] By these accounts, geostrategic competition *within* cyberspace is characterized by networked relations, but the extent to which this implies a shift from 'modernist' type geopolitics (i.e. interstate interactions, structured by geography and technological variables) remains debated.

Tensions and limitations

Significantly, emphasizing the 'unique' networked character of cyberspace runs the risk of isolating the domain from its wider context, thus overlooking cyberspace's integration with other policy areas, infrastructures, and technologies—and the potential consequences for dynamics of geostrategic competition. Overlooking these relations obscure, as Klinke puts it, 'how power operates above and beneath hegemonic cartographies of state power' (2021, p. 356).[15]

[14] While there are elective affinities between the spatial logic of modernist accounts and structuralist, networked approaches to the cyber domain, most networked accounts reject the 'fixity' and associations with classical Euclidean and/or cartographic space, and they dispel traditional calculations of proximity and distance (e.g. the LSG). Further, some accounts which have adopted ANT concepts (e.g Dunn Cavelty & Balzacq, 2016) further challenge notions of classical geopolitics which treat 'spaces as a pure container for objects', approaching actors and objects as co-constitutive of space (see Balzacq & Dunn Cavelty, pp. 183-184 for further discussion; see also Lambach, 2020 for a critique). Other approaches to Actor Network Theory adopt a more radical view, approaching geography as 'connectivity not space' (for discussion see O Tuathail, 1998, pp. 24-25; Latour, 1996; Barder, 2019).

[15] A similar criticism has been levied towards classical geopolitics accounts (see Klinke, 2021 for a full discussion). While this criticism of 'flattening' may not reflect the full range or diversity of geopolitical thought, popular imaginations of 'cyber geopolitics' have yet to fully examine the sociotechnical (and geostrategic) consequences of cyberspace's convergence with other domains of power.

In particular, networked ontologies of cyberspace have struggled to integrate relevant insights about geopolitics from other adjacent areas of IR scholarship, such as political geography and international political economy (IPE). Engaging this wider literature reveals the limitations of conceiving of cyberspace through a relatively flat ontology. These literatures have demonstrated that networked hierarchies in and through cyberspace have *variably* reinforced or challenged extant power balances in the global system (Lehdonvirta, 2022; Pohle & Voelsen, 2022; Drezner et al., 2021). Rather, networked approaches have tended to emphasize the compression of space, geography, and time (*deterritorialization*) without paying equal attention to processes of *reterritorialization* in and through cyberspace.[16] By 'juxtapos[ing] the decentralized, spatially dispersed web with the containerized territorial state,' Lambach argues, such approaches have 'treated the internet as a deterritorializing force,' (2020, p. 488). Such an artificial comparison reproduces what Agnew calls the 'territorial trap' in IR literature, in which 'geographical division of the world into mutually exclusive territorial states […] has served to define the field of study,' (Agnew, 1994, p. 53).

Significantly, while the 'virtual' and/or logical layer of cyberspace may be characterized by decentralized networks, the 'physical' and 'hardware' components of cyberspace are integrated with other digital infrastructure and technologies. These accounts reveal a 'pluralization of power' and dynamics of asymmetric interdependence, evidenced by the centralization of power over transoceanic submarine cables (which form the internet's 'backbone') (Gjesvik, 2023); the monopolistic evolution of ICT carrier services (Rühlig,

[16]Notably, networked ontologies *and* classical geopolitical thought can be accused of 'flattening' relations of geopolitics into 2D space, thus failing to explore their *vertical* integration in and through other domains and materialities—or obscuring, as Klinke puts it, 'how power operates above and beneath hegemonic cartographies of state power' (2021, p. 356). This is particularly relevant to cyberspace, given widespread recognition of the complications it poses to traditional state territoriality and sovereignty. While this criticism of 'flattening' may not reflect the full range or diversity of geopolitical thought (see for example Klinke, 2021), popular imaginations of 'cyber geopolitics' have yet to fully examine the sociotechnical (and geostrategic) consequences of cyberspace's convergence with other domains of power.

2023), and the development of state 'intranets,' (Chander & Sun, 2021). Therefore, scholars have emphasized that, while states are seen to 'engage in indirect forms of rule, such as delegating to or orchestrating the activities of intermediaries,' it should not be assumed that there are no hierarchical relations *within* or *across* networked layers of cyberspace (Lambach, 2020, p. 486).

In sum, networked ontologies of cyberspace suggest that geostrategic competition *within* cyberspace is characterized by fluid spatial and temporal dynamics, as well as conditions of technological interdependence. The distinctive environmental features of cyberspace, including its complex territoriality and temporal features, and the semantic features of cyberspace—including its low entry barriers for cyber disruption—have raised questions about whether cyber operations could 'revolutionize' the nature of competition and conflict (Kello, 2013). Notwithstanding their insights, relying upon these conceptions alone leaves out important dimensions of geostrategic competition relevant to cyberspace—particularly its integration with the wider strategic context. As Foulon and Meibauer put it, such an approach 'risk[s] ignoring how cyberspace interacts with other dynamics of international relations,' (2024, p. 430).

2.2.2. Systemic level: Realism, capabilities and structural factors

Meanwhile, a burgeoning body of literature in security studies has taken further steps to explore how cyber operations, and cyberspace as a domain, factors into global dynamics of competition (e.g. Buchanan, 2020; Kello, 2022; Betz & Stevens, 2011). Rather than approaching cyberspace as a distinctive (and isolated) domain, this literature has examined cyberspace from a wider, systemic perspective—as a factor which shapes the 'rules of the game', or international structure (Foulon & Meibauer, 2024). For example, in our

contemporary era of ‘unpeace’, Kello (2023) holds, ‘intensifying geopolitical competition beyond cyberspace provides growing motives for unpeaceful activity within it,’ (p. 124).

Valuably, this scholarship has sought to integrate IR scholarship more closely with cybersecurity studies (e.g. Kello, 2013; 2017; Foulon & Meibauer, 2024), and it has played a prominent role in shaping policy debates about the strategic provenance of cyber capabilities for broader escalation dynamics (e.g. Lonergan & Lonergan, 2023), and the effects of cyber operations on the battlefield (e.g. Rid, 2022; Kostyuk & Gartzke, 2023). Scholars in this vein have likened contemporary competition in and through cyberspace to older playbooks of ‘wiretapping’ and ‘information shaping’ (Buchanan, 2020; Kello, 2022).

Alike ‘domain-level’ approaches, scholars examining these dynamics from a wider lens have also underscored networked dynamics as characterizing global relations in and through cyberspace, including sovereigntist behaviour (e.g. Choucri & Clark, 2018). For example, Betz and Stevens observe that,

> ‘Parts of traditional government hierarchies have been networked within and across states in order to assert authority and control […] In these networks may perhaps be found the future of the state: one in which further aspects of sovereignty are relinquished in order to retain authority, control and, importantly for governments and rulers, relevance,’ (2017, p. 74).

In this vein, scholars have argued that revisionist global powers are able to exploit the legal ambiguity surrounding the use of cyberespionage, thereby pursuing asymmetric information advantages under the guise of plausible deniability and avoiding the risks of military retaliation (Dunn Cavelty & Wenger, 2022). Under these conditions, Kello (2023) argued that

> ‘the main goal is not to seize geographic territory (how could intangible zeros and ones do that?) or even to coerce state behaviour. Rather, the primary goal is to weaken the internal political bases of adversaries’ foreign and security policy, thereby diminishing its assertiveness and effectiveness,’ (p. 124).

By contrast, other accounts have emphasized that securing advantage *through* the ownership and control over digital infrastructure and technologies—thereby enabling cyberespionage or strategic leverage—has become a primary axis of US-China strategic competition (Farrell & Newman, 2019; Buchanan, 2020; Lehdonvirta et al., 2025). For instance, undersea fibreoptic cables—which transport 97% of all global data (including both civilian and military communications)—have multiple global chokepoints that are considered highly vulnerable to state coercion and exploitation (Bueger et al., 2022; McGeachy, 2022). Under conditions of increased economic interdependence and rising costs of conventional warfare, scholars have argued, seeking asymmetric influence through cyber means has only become more attractive (Baezner & Cordey, 2022). As I discussed at the beginning of this chapter, varied conceptions of territorial control through cyberspace could be due to varying conceptions of cyberspace an environment.

Significantly, the majority of this scholarship has tended to rely upon classical IR theories of power premised upon Westphalian territorial assumptions (Kello, 2017), particularly realism (e.g. Foulon & Meibaurer, 2024; Buchanan, 2020), to explain power relations in and through cyberspace (albeit with exceptions; notably Betz & Stevens, 2011; Dunn Cavelty & Wenger, 2022; McCarthy, 2015).[17] Dominant accounts have emphasized the significance of network positioning, cyber capabilities, and technological prowess as key determinants of states' geostrategic behaviour in the digital age. According to traditional realist thinking, state power is conceived as state assets, or *capabilities,* including material resources, industrial capacity, military might, and population (Morgenthau 1948, pp. 80-108). Adapting these assumptions to cyber-IR, scholars have emphasized the significance of

[17]Classical geopolitical theorists such as Halford Mackinder recognized the importance of material capabilities and the balance of power, whereby changes in weapons and transport technologies served as 'dynamic factors' which mediate the relationship between strategy and geography (Gray & Roan, 2011). See also Zakaria (1998, pp. 181-183) for a discussion about realist thought and American expansionism. Refer to the section 'Modernist geopolitical thought and its relevance to IR' for further details about the basic assumptions of realism.

cyberwarfare capabilities or 'cyber weapons' (i.e. offensive and defensive cyber capabilities) and a strong intelligence arm for exercising cyber power (Gartzke & Lindsay, 2016; Cai, 2018; Douzet, 2014; Kello, 2017).[18] Other 'hard power' resources, including the ownership and production of critical technologies, are also viewed as key determinants of power (Slayton, 2016).

Drawing upon these characteristics, mainstream IR accounts of geopolitical competition over cyberspace have generally positioned the US and China as powerful opponents in a techno-geopolitical struggle over and through cyberspace (Weber, 2020). In this way, cyber*space* is often bifurcated into two competing technological spheres of influence, within which an external (American or Chinese) power exerts control over the sphere's technology, and therefore its existence to a large degree.

Despite the influence of realist thinking in understanding dynamics of geostrategic competition in and through cyberspace, there is no shared definition for cyber power in the realist paradigm (Craig & Valeriano, 2018). In particular, the bulk of scholarship on geostrategic competition through cyberspace has revolved around debating the effects of cyber capabilities and material technological advantages.[19] Below, I review a prominent debate in cyber-IR scholarship on competition to illustrate the theoretical and empirical limitations to privileging cyber capabilities to predict and explain dynamics of geostrategic competition. These shortfalls, I subsequently argue, reveal empirical and theoretical blind spots about geostrategic behaviour in and through cyberspace.

---

[18] Common examples of 'cyber defensive' capabilities include firewalls, encryption, and intrusion detection software. Examples of 'cyber offensive' capabilities may include exploits (e.g. Zero Days, or unknown cybersecurity vulnerabilities); spyware, and malicious code (e.g. ransomware). However, the distinction between cyber offensive and defensive capabilities is heavily debated (see for example Valeriano, 2022).

[19] As McCarthy argues, the IR field's 'stress on technology as one of the material resources that define power – the only shared characteristic across disparate Realist conceptions of power– has, in many ways, defined our understanding of technology as a form of power in global politics' (2015, p. 528).

Cyber capabilities, strategic advantage, and strategic competition

The provenance of cyber capabilities for international conflict and competition has bearing upon two foundational ideas in international security literature: *offence-defence* balance theory (ODB), and by extension, incentives to compete or cooperate under anarchy. Competition is widely understood as a defining characteristic of interstate behaviour under conditions of anarchy (Fearon, 2018; Blagden, 2021). According to realist thinking, whether or not competition manifests as military conflict (war) depends on offence-defence calculations, whereby the relative ease of conducting attack or defence is mediated by prevailing military technology 'taken in its geographical context,' (Blagden, 2021, p. 1). Specifically, the more military technology and geography favour the offence, there is reduced potential depth of interstate cooperation (Jervis, 1978; Fearon, 2018). In other words, 'deeper cooperation is possible when the odds of successful attack are lower for any given force levels,' (Fearon, 2018, p. 541). Manipulation of the offence-defence balance, then, can affect adversaries' perceptions of whether they can resort to military conflict at 'acceptable relative cost' to pursue their strategic objectives (Blagden, 2021, p. 20).

Since theories of the offence-defence balance are often premised upon the intrinsic properties of technologies or technological systems as improving the relative ease of defence or offence, cyber capabilities and their relationship to global stability remain a rich area of debate (Slayton, 2016, p. 76). As Slayton surmised, the utility of cyber offence according to ODB would be 'the value of the offensive goal (e.g., taking territory, stealing secrets, or gaining control of a computer) less the minimum costs of achieving it; the utility of the defence is the value of the defensive goal (e.g., holding territory, maintaining secrecy, keeping control of a computer) less the minimum costs of defence,' (2016, p. 80). Proponents of cyber capabilities favouring the offensive side have highlighted the higher technical, financial, and temporal costs of defending entire networks (compared to the lower costs of

exploiting a single network vulnerability). Given that contemporary systems are increasingly dependent on such technology, cyber-attacks can promise the 'strategic decapitation' of military command and control systems (Lieber, 2014, p. 96). As Gartzke notes, 'If powerful developed nations largely immune to terrestrial onslaught can have their defences disabled and their factories idled by foreign hackers, then perhaps "Pearl Harbor" is an appropriate metaphor,' (2013, p. 42).

However, measurement and conceptualization challenges have rendered ODB's operationalization in the cyber context controversial, both in academic and policy circles. Put simply, cyber capabilities exacerbate one longstanding critique of ODB: the model is notoriously difficult to empirically operationalize (Lynn-Jones, 1995; Lieber, 2014). As Gartzke points out, 'advocates [of cyber offence] have yet to work out how cyberwar enables aggressors to accomplish tasks typically associated with terrestrial military violence,' (2013, p. 42). Indeed, proponents of cyber defensive advantage have argued that cyber threats—and their implications for the offence-defence balance—have simply been overblown (Gartzke, 2013). Separately, Slayton asserts that offensive advantage in cyberspace is based upon false assumptions about the intrinsic ('revolutionary') properties of technologies or technological systems (2016, pp. 87. 91). This debate points to a larger measurement challenge for scholars building databases about cyber conflicts and tracking the development of cyber capabilities: scholars cannot be certain as to whether they are capturing the full scope of the 'main incidents' in cyber conflict and/or whether they are observing the most up to date capabilities at actors' disposal (Lupovici, 2022).

Notably, cyber capabilities are often not publicly visible (unlike tangible conventional weapons), which makes it difficult to identify a state's capabilities and their record of using them (Moore, 2022; Stevens, 2018), and high-yield cyber weapons are transitory and often single-use (Smeets, 2022). It has recently been agreed that the most

effective cyber campaigns—and the use of cyber power—are often invisible and undetectable to the victim (see Buchanan, 2020; Moore, 2022). As Stevens observes, the 'immateriality [of cyberweapons] complicates their practical identification and interdiction, and also because all existing legal regimes recognise weapons as material entities,' (2018, p. 493).

Even when detected and patched, cyberattacks are typically plagued by attribution problems, therefore obscuring the wielder of cyber power (Egloff, 2019). These empirical trends have led to a tendency for cyber actors to hoard multiple zero-day exploits (indeed for years), therefore leading to a cache of unused cyber capabilities (Smeets, 2022). In fact, the 'intangible' nature of cyber operations has spurred a growing trend in scholarship to liken 'cyber' to an intelligence contest (Chesney & Smeets, 2023) or as a tool for shaping (Buchanan, 2020) rather than a collection of punctuated cyberattacks as the proxy for cyber capabilities.

Overall, cyberspace is an imperfect fit for the ontological underpinnings of the ODB debate and other classical accounts of power politics which rely upon fixed geographic conditions and military capabilities. To the author's knowledge, the literature does not have a clear conceptualization of cyber capabilities and their distinction from related concepts as 'cyber capacity',[20] nor does it have shared agreed about the distinction between 'defensive' and 'offensive' cyber capabilities (Valeriano, 2022). Since cyber capabilities could potentially be deployed to achieve a multitude of strategic and operational goals (Buchanan, 2020) and given the difficulties distinguishing between offensive and defence cyber activities, relying upon cyber capabilities to predict and explain strategic behaviour is insufficient. Indeed, scholars seeking to understand cyber deterrence face similar challenges to the ODB debate: they struggle to access information to cases of cyberattacks, and

[20] I elaborate upon this point in the final section of the chapter.

attribution problems raise questions about whether a credible deterrence strategy had been employed (and perceived) by adversaries (Lupovici, 2022; 2021), particularly in terms of signalling (Buchanan, 2020).[21]

The debated strategic utility of cyber capabilities raises empirical and theoretical questions about why actors have continued to integrate cyber and digital instruments into their foreign policy objectives and strategic doctrines, particularly in the context of geostrategic competition.

Cyber capabilities and interstate geostrategic competition

Despite their weak independent strategic utility, scholars have argued that cyber operations remain attractive to both powerful and weak state actors for various reasons. On the one hand, cyber operations can enable great powers to compete below the threshold of all-out war, thereby avoiding the risks of destabilizing the overall system (Buchanan, 2020; Kello, 2022; 2023). Weak actors are held to profit from the low entry barriers and accessibility of cyberspace to facilitate 'grey zone operations' and/or 'hybrid' warfare (Nye, 2010, p. 4). More broadly, 'cyber' tools have become perceived as an enabler for broader strategic goals, as seen with debates on the importance of 'cybersecurity' for digital sovereignty and strategic autonomy (Bellanova et al., 2022).

Other rationalist accounts have explained the integration of 'cyber' into (geo)strategic doctrine as being incentivized by pressures for military modernization (and technological advantage), given that militaries have become increasingly reliant on cybersecure command and control systems (Lindsay & Gartzke, 2020). Since constructing technologies in specific operational domains confers different comparative strategic advantages, the technological

[21] Note that Buchanan (2020) argues that the 'shaping' effects of state behaviour in cyberspace are much more discernible and significant, compared to signalling effects (both of which may be considered within a classical deterrence framework).

modernization process fundamentally exposes the trade-off between 'guns and guns' that today's strategic decision makers face, between procuring and maintaining different types of strategic capabilities (Lindsay & Gartzke, 2020, p. 746). This is an astute yet difficult to operationalize point, given that the strategic utility of cyber operations remains debated, and cyber capabilities can often serve multiple strategic objectives.

Scholars have also speculated as to whether cyber capabilities are attractive to develop on the basis of prestige (Khong, 2019). However, if prestige is the 'shadow cast by [hard] power', particularly military power (Acheson, 1969, p. 405), classical 'prestige' scholarship is limited in explaining the role of cyberspace in contemporary strategic competition, particularly outside of the 'major (state) powers.'[22] As outlined above, cyber capabilities cast a transient shadow, if at all: they are not as 'flashy' as classical 'prestige weapons' and their procurement is often concealed. Further, prestige is dependent on social recognition, and it is relative: the 'political consequences of attributing prestige influence the attribution of prestige' (Mercer, 2017, p. 141). Yet, the emotional and/or symbolic effects of 'offensive cyber weapons' remain controversial. As Smeets and Lin write, the 'symbolic value as a 'prestige weapon' to enhance 'swaggering' remains unclear, due to its largely non-material ontology and transitory nature,' (2018, p.55).

Summary

Overall, the bulk of cyber-IR scholarship on (geopolitical) competition in and through cyberspace, often positioning itself in international security studies debates, has tended to adopt a realist orientation to debate the strategic promise of cyber capabilities and their

[22] There are further empirical limitations pertinent to my study: as prestige-based explanations tend to be centred upon traditional 'great powers' and their material capabilities, they are also limited in explaining the EU's embrace of geopolitics and its desire to emerge as a 'leader' vis-à-vis the US and China (as explored in Chapters 4-6). If the concept of prestige is reliant upon 'military capabilities' and 'voluntary deference' as some scholars contend (e.g. Mercer, 2017), it cannot easily grasp one of the key sources of EU power—the Brussels effect—which is based upon its regulatory and economic might, not only normative power.

relationship to interstate competition and conflict. By privileging cyber capabilities in debates about competition and conflict, as evidenced by debates about ODB in cyberspace, some scholars have argued that the realist literature employs "the concept [of cyber power] programmatically…making implicit assumptions about what strength in the cyber-domain means, but without substantiating them,' (Dunn Cavelty, 2018, p. 317; see also Slayton, 2016).

Furthermore, the field of cyber-IR, particularly international security, has focused heavily upon traditionally powerful nation-state actors such as the United States (US), Russia, and China, and 'rogue' states such as Iran and North Korea (Valeriano, 2022; e.g. Kello, 2017; Weber, 2018; Smeets, 2022; Moore, 2022; Buchanan, 2020).[23] Even 'networked approaches', which have emphasized the erosion of Westphalian territoriality, have focused upon interstate competition in and through cyberspace (see also Branch 2021; 2024; Lambach, 2020; Cristiano et al., 2023, p. 332). To be sure, the early development of the internet ('ARPANET') was shaped by United States and its Cold War rivalry with the Soviet Union, and its expansion through undersea cables were initially owned by national governments (Choucri & Clark, 2018; Gjesvik, 2022). However, the ownership and control over key dimensions of cyberspace—and the actors involved in geostrategic competition in this context—have expanded and diversified over time (Nye, 2014; Choucri & Clark, 2018; Sukumar et al., 2024).

While states are undoubtedly key actors in dynamics of geostrategic competition, these studies have left open several significant gaps in our knowledge about the multifaceted

[23] Cyber studies of international security often examine how states interact, sponsor, and/or mobilize hacker groups to shape the environment (Buchanan, 2020; Moore, 2022), as well as the development of cyber capabilities by militaries for strategic objectives (Lin & Smeets, 2018; Smeets, 2022; Chesney & Smeets, 2023). For example, see Kello's seminal work, *The Virtual Weapon* (2017), which advocates for a closer synthesis between cyber studies and international security studies, with a focus on predicting and understanding interstate behaviour (p. 29). Indeed, the debate on deterrence, coercion, and escalation in and through cyberspace is squarely concerned with state behaviour (see for example Chesney & Smeets, 2023; Maschmeyer, 2023; Lonergan & Lonergan, 2023; Lindsay & Gartzke, 2016; 2020).

practice of geopolitics in and through cyberspace and the diversity of actors involved in it.[24] Notably, an emerging body of literature has established that claims to centralized control and influence over digital networks are not confined to state actors and their interactions with cyber threat groups (Broeders et al., 2025; see also Smeets, 2025). Contributions from IPE scholars have underscored that the expanding nature of cyberspace has provided new opportunities for private actors and states alike to reconstitute the distribution of power across interdependent global networks (e.g. Lehdonvirta, 2022; Drezner et al., 2021; Kokas, 2022). In this context, geospatial concepts have emerged in the vocabularies of supranational actors and the private sector, and they have shaped the policy practices of global actors such as the European Union (see for example Barrinha & Christou, 2022; Sukumar et al., 2024; Microsoft, 2025).

Critically, we know very little about how these actors engage in geostrategic competition and whether dominant assumptions about the determinants of geostrategic behaviour in and through cyberspace (e.g. cyber capabilities, military force, and technological prowess) may apply to less conventional contexts. As I sketch out below, the theoretical limitations of extant approaches to geostrategic competition are illustrated by the field's inability to sufficiently explain and predict the EU's emergence as an ambitious geopolitical and sovereigntist cyber actor.

Capabilities, interstate competition, and the puzzling case of the European Union

As the 'technological crescent' over which the United States and China struggle for dominance, mainstream cyber-IR accounts framed the EU as unable and *unfit* to pursue geopolitical interests (Weber, 2020; see also Sliwinski, 2014). Consequently, realist and

[24] Therefore, my point is not that states have become irrelevant or substitutable by other forms of political organizations in the context of geostrategic competition, but that we should widen our focus beyond the territorial state. For a broader discussion on this, see Ruggie (1993, p. 140-145).

state-centric approaches emphasizing cyber capabilities and Sino-American competition failed to anticipate and explain the EU's embrace of 'digital sovereignty' and the Commission's overall mission for 'the EU [to] learn the language of power and act geopolitically,' (Weiler, 2020; e.g. Sliwinski, 2014; Howorth & Menon, 2009). After all, the EU lacks the material military or intelligence capabilities to conduct cyber warfare, and it is not a (sovereign) territorial state.

Defying realist skepticism about the EU's capacity to hold and articulate geostrategic ambitions, the EU has positioned itself as an aspiring global cyber actor, both in terms of discourse and practice (Bellanova et al., 2022; Falkner et al., 2024). While the Union 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' (Haroche, 2023). Further, despite its well-documented 'capabilities-expectations gap' (Hill, 1993), the EU has also advanced its own policies and development projects into geopolitically significant regions, exemplified by its funding of 'CyberEast' programmes in its Eastern Neighbourhood and its more ambitious 'Digital Europe' programme, which includes a range of financing and projects relevant to cybersecurity, digital infrastructure, and digital technologies. Accordingly, the EU has been likened to a 'digital hub' alongside the United States and China (Drezner et al., 2021), and a 'digital empire', as well as an ambitious global cyber actor (Bradford, 2023).

Arguably, extant materialist and realist approaches to *explaining* the EU's geostrategic behaviour in and through cyberspace also fall short.[25] Mobilizing neorealist theory, one could argue that the EU's geostrategic behaviour is an *emulation* of its strategic

[25] N.B. I explore these debates in more detail, with further reference to EU Studies scholarship, in Chapters 4 and 6.

rivals and/or competitors, the United States and China. By this 'Waltzian logic' of emulating great power behaviour, the defining characteristics of the EU's geopolitical turn would be *imported* into EU policy processes, as predominantly a 'counter-move' to geopolitical rivals (Haroche, 2023).

While the EU has indeed positioned some of its recent initiatives as 'alternatives' to Chinese and American policy packages, including in the area of digital development, scholars have instead pointed to an *internal* geopolitical logic *within* the context of EU policymaking as shaping the EU's responses to the international environment (Costa & Barbé, 2023). Furthermore, emulation cannot adequately account for the other capstone of the EU's 'geopolitical Commission': the EU's digital sovereignty agenda. In advancing 'European digital sovereignty claims', Brussels has explicitly sought to differentiate itself from China's version of '*cyber* sovereignty,' and the United States, which has not advanced a clear position on digital sovereignty (Kokas, 2022). Overall, while the EU may be competing with the US and China, Brussels has not been consistently *conforming* to the models of either Washington or Beijing.

For similar reasons, the European integration theory of *intergovernmentalism*, an approach which may be included within the realist paradigm (Hix, 1994), also struggled to anticipate the EU's geostrategic turn. 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 (Hoffmann, 1996; Hix, 1994). By this account, the EU's policy development is the reflection of Member States' pooled sovereignty and diverse national interests (Hoffmann, 1996). Adopting this approach, Sliwinski argued that dynamics of pooled sovereignty would constrain the EU's capacity to develop an assertive role for itself as a cybersecurity actor due to inconsistencies between national security narratives, and 'traditional sovereignty claims are more than likely

to leave the EU toothless in the future,' (2014, p. 470). Sliwinski's (2014) explanation therefore did not anticipate the EU's invocation of European sovereignty in its most recent strategy, as he argued that 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'.

A state-centric, intergovernmentalist focus could not adequately account for the emergence of EU-specific norms and interests in the EU's cyber strategy (see also Farrand et al., 2024; Haroche, 2023), including 'European digital sovereignty' discourse. For one, the EU is not a traditional Westphalian foreign policy actor (Gravier, 2011; Fossum, 2006). Rather, 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,' (Sjursen, 2011, p. 1089). This is laid bare by the fact that, at the time of the release of the first EU-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 (Pawlak, 2018; Klimburg & Tirmaa-Klaar, 2011). 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,' (Trimintzios et al., 2017, p. 5). This contravenes the intergovernmentalist assumption that national governments are the sole drivers of EU-level cybersecurity policy.[26]

Lastly, domain-level approaches to cyberspace have emphasized the complications cyberspace poses to Westphalian (nation state) territoriality. However, the pursuit of sovereigntist logics *through* cyberspace as a dimension of geostrategic competition has been less discussed by mainstream cyber-IR scholarship. This may be due to the fact that, from a systemic perspective, territorial sovereignty is an attribute shared by all nation states engaging in geostrategic competition. This perspective elides the significance of

[26] Refer to Chapter 3 for further elaboration on the EU cybersecurity policy context.

sovereigntist behaviour pursued by non-conventional global cyber actors such as the EU (or indeed 'Big Tech' companies). As sovereignty 'is expressed spatially' by geopolitical agents in terms of *territorial* control and *functional* control over space/virtual communities (Eudaily & Smith, 2008), the EU may be seen to claim authority over the territorial/functional control of the 'European' digital domain and to express its desire to play a particular geopolitical role in the global digital environment (Floridi, 2020). Further, the articulation of sovereignty claims within the context of geostrategic competition can be understood to challenge or muddy the distinction between nation states from other global actors in and through cyberspace.

Failing to capture these dynamics may be due to the 'sovereignty paradox' in classical IR thinking: whereby sovereignty (nation-state) territoriality is approached 'as a necessary condition for [the state's] ability to articulate power; however, this territorial imperative must first be satisfied by some sovereign legitimate authority,' (Eudaily & Smith, 2008, p. 314). By advancing European spatial logics towards global cyberspace, the EU's geostrategic claims challenge both modernist geopolitical accounts premised upon the classical nation state and postmodernist, networked-based ontologies of cyberspace, which have often downplayed sovereign territoriality as a spatial ordering principle.

2.2.3. Section summary

Collectively, mainstream scholarship has paved the way for further exploring the convergence—or 'the mutually intrusive interdependence' of cyberspace and international relations at large (Choucri & Clark, 2018, p. 268). The convergence of cyberspace with geostrategic competition illustrates this 'co-evolution', introducing further complexities and tensions to classical notions of geopolitics. However, mainstream IR literature has largely characterized geostrategic competition in and through cyberspace as occurring between

nation states, whereby interstate behaviour is conditioned by the possession of cyber capabilities and a state's favourable positioning in a networked environment.

Notwithstanding its valuable contributions to cyber-IR, mainstream accounts have several theoretical and empirical limitations, leaving gaps in our knowledge about the emergence, drivers, and characteristics of geostrategic competition in and through cyberspace. As I illustrated with the case of the EU, geostrategic competition *in practice* has a wider scope than the primary foci of mainstream framework. Given these conceptual challenges and the research objectives of my study, which focuses upon the EU's geostrategic turn in and through cyberspace, it is worthwhile to turn to critical geopolitics approaches and constructivist research.

Below, I consider how critical scholarship offers further opportunities to bridge the gap between theoretical approaches to geostrategic competition in and through cyberspace, and empirical reality. It also provides further analytical tools for assessing the 'double nature' of geostrategic concepts as categories of (academic) analysis and categories of practice (lived experience).

2.3.1. Critical scholarship: Geopolitical imaginaries and sovereigntist logics in and beyond the nation-state context

Critical and constructivist scholarship has paved the way for a multifaceted, sociotechnical approach to examining the co-evolution of cyberspace and geopolitical behaviour in cyberspace. According to critical geopolitics approaches, geopolitics is approached analytically as a question, rather than a set of fixed material (and territorial) variables (Kuus, 2014; see also Ó Tuathail & Agnew, 1992; see also Lambach, 2020). Valuably, such an approach invites us to ask why cyber capabilities are perceived as geostrategically advantageous and to problematize how and why policymakers construct

cyberspace as a (geo)strategic domain in particular ways, including the possibilities of other policy tools or 'solutions' for pursuing geostrategic goals.

Broadly, constructivist accounts emphasize the socially constructed and ideational dimensions to strategic decision-making in and through cyberspace. Accordingly, they have contributed a rich literature to cyber-IR about the 'securitization' of cyberspace (see for example Hansen & Nissenbaum, 2009; Balzacq & Dunn Cavelty, 2016; Christou, 2016, 2019; Gomez & Whyte, 2021; Cristiano et al., 2023; Carrapico & Farrand, 2020; Cruz Lobato & Kenkel, 2015). Indeed, s*ecuritization* is one of the most prominently featured concepts in IR literature about discursive dynamics in cyberspace (Balzacq & Dunn Cavelty, 2016). It is classically understood as political elites' discursive construction of particular objects as existential threats to survival through a 'speech act,' which can open up new pathways and rationalities for action in line with the 'politics of emergency,' (Buzan & Wæver, 2003).

Particularly relevant to this thesis project, discourse-oriented work has documented the rise of geopolitical, sovereigntist, and spatial metaphors to legitimize the extension of state and/or regulatory control into cyberspace (e.g. Betz & Stevens, 2013; 2017). This global shift has been characterized by a move from purely technical and securitized narratives towards geopolitical and sovereigntist assertions. For example, policymakers have leveraged metaphors such as the 'Digital Cold War' as a heuristic device to approach the complexity of cyberspace (Chander & Sun, 2021), although such analogies have been deemed as inadequate representations of cyberspace (Betz & Stevens, 2013).

Critical geopolitics scholarship holds that, since 'sovereignty is expressed spatially,' this conceptualization serves as 'an insertion point for [critical] geopolitical analysis' (Eudaily & Smith, 2008, p. 312). Similarly, challenging traditional 'modernist' approaches to sovereignty in IR, constructivist scholarship on 'digital' and/or 'cyber sovereignty' has

demonstrated how sovereigntist claims do not adhere to a neat Westphalian logic in cyberspace (Lambach, 2020; Pohle et al., 2024).[27] For one, 'digital sovereignty' claims are often practically overlapping or 'pooled' with other political entities (Bellanova et al., 2022). Additionally, other 'digital sovereignty' initiatives, such as Estonia's 'cloud sovereignty' approach, have sought to establish the government's 'system[s] of rule' (Ruggie 1993, p. 148) beyond its territorial borders.[28]

Meanwhile, other scholars have argued that claims to 'digital sovereignty' have emerged as a *discursive practice*, premised upon two dominant ways of thinking about cyberspace: 'cyber exceptionalism' and 'internet governance' (Pohle & Thiel, 2020). 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 (and therefore the need to restore it), the latter encompasses the multistakeholder model, wherein states have 'different and non-sovereign roles' as regulators in collaboration with other stakeholders (Pohle & Thiel, 2020, p. 2). Exemplifying the former approach, Beijing and Moscow advocate 'Internet sovereignty' or 'cyber sovereignty' at the international level as a way to preserve their domestic authority and control in cyberspace from encroachment (Stevens, 2018, p. 495; see also Zeng et al., 2017). Contestation and competition over the establishment of cyber norms, including about state sovereignty, have been characterized by polarization in formal internet fora, complex governance regimes, and diplomatic lobbying by non-state actors (Sukumar et al., 2024; Choucri & Clark, 2018; Raymond & Sherman, 2023). These sociopolitical developments challenge traditional renderings of territorial

[27] 'Modernist' accounts of territoriality in IR have long been challenged by constructivist and critical scholarship. See for example Ruggie (1993); Agnew & Corbridge (1989); Ó Tuathail (1998).
[28] Estonia's concept of 'cloud sovereignty' serves to back up the government's e-governance networks in case it loses territorial independence. Tallinn's 'Data Embassy' is physically outside of Estonia's territorial borders, but it remains 'under Estonian state control'. See Rice (2019) and e-Estonia (n.d.).

sovereignty, geopolitical expansion, and strategy as being naturally tied to nationally defined geographic conditions (Stevens, 2018; Betz & Stevens, 2011).[29]

These insights help us to move beyond the limitations of mainstream domain- and system-level characterizations of geostrategic competition in several ways. Foremost, such approaches emphasize the '*the production of space*'—that is, 'how places are socially and materially created, reconfigured and experienced' in various contexts (Cloke, Crang, & Goodwin, 2014, p. 940; in Weaver, 2020, p. 2). By this account, spatial (b)ordering practices—including in cyberspace—do not necessarily reproduce traditional territorial state boundaries. Rather, they can also offer new possibilities for actors to reform existing modes of global spatial order (see also Mueller, 2020; Branch, 2024, p. 310). In other words, this approach asks us to approach geostrategic behaviour not on the basis of capabilities, but in terms of 'spatial (b)ordering practices'—that is, *producing* and *demarcating* space through ideas, practices, and institutions (Lambach, 2020; Branch, 2024; see also Simmons & Hulvey, 2023).

Second, this approach provides new analytical tools for understanding *why* actors have adopted geostrategic behaviours in the context of cyberspace along several lines. Critical geopolitics scholars emphasize the significance of a 'geopolitical imaginary' for shaping an actor's approach to a particular context (e.g. Branch, 2024). A *geopolitical imaginary* is a particular cognitive framework of existing practices and spatial understandings of an environment (Clark & Jones, 2011). Beyond the context of cyberspace, scholars have demonstrated how a '*geopolitical imaginary'* acts as a stabilizing framework of reference

[29] As Stevens notes, however, from a Krasnerian (1999) perspective, cyberspace does not challenge various expressions of sovereignty equally. As Betz and Stevens (2017) argue, given that the internet does not impinge upon states' sovereign equality under international law, *international legal sovereignty* is scarcely affected (see also Stevens, 2018). By contrast, *interdependence sovereignty* (the capacity to control borders), *Westphalian,* and *domestic sovereignty* are potentially violated by the difficulties of managing and controlling transnational data flows, and by disruptive cyber operations which interfere with a state's internal affairs, such as politically targeted disinformation and malware (Stevens, 2018; see also Broeders et al., 2023).

upon which actors draw to make sense of the unfamiliar spatial environment (Clark & Jones, 2011; Kuus, 2014; Eberle & Daniel, 2022). Accordingly, strategic ambiguities and perceived insecurities can encourage political actors to fall back on familiar 'cognitive maps' and geospatial analogies (see also Betz & Stevens, 2013).

Third, critical geopolitics approaches provide us with further opportunities to scrutinize the relationship between sovereignty claims and geostrategic competition. Critical geopolitics scholars have argued that modernist accounts approach territorial sovereignty as a dispositional feature of geopolitical behaviour. In so doing, modernist approaches collapse the potentially mutually reinforcing logics of sovereignty and geopolitics as distinct but interrelated spatial ordering principles—thus eliding the significance of sovereignty as a legitimizing concept for geopolitical behaviour. As Eudaily and Smith contend, in international politics, conceiving of 'geopolitics without sovereignty leaves us only with artificial states and crocked lines left to be filled in, described, apportioned, reapportioned, united, divided, and redivided,' (2008, p. 313). By foregrounding how sovereignty and geopolitics may serve as *potentially* mutually constitutive 'geostrategies' or 'spatial ordering logics' in theory and practice, we can gain a more complete and multifaceted understanding of geostrategic competition in and through cyberspace.

Overall, critical approaches offer several promising tools to approach geostrategic competition in and through cyberspace. However, this literature has often occupied peripheral positions in mainstream IR literature debates about 'cyber geopolitics', or it has tended to avoid direct engagement with the field's dominant assumptions (i.e about states and cyber capabilities as the key variables of interest).[30] Critical geopolitical perspectives,

[30] There are, of course, exceptions, including: Dunn Cavelty and Wenger's (2022) volume; Balzacq & Dunn Cavelty (2016); Stevens (2018); Lambach (2020, 2024) and Branch (2024). My research hopes to build upon their contributions.

albeit with some exceptions, have tended to engage more closely with political geography literature (cf. Lambach 2020; Branch 2020, 2024), rather than mainstream IR debates.

Further, while constructivist work has offered pathbreaking contributions to IR about the *securitization* of cyberspace and cyber norms from a global governance perspective, there remains significant scope to leverage constructivist tools to understand the *geopoliticization* of cyberspace. Given that these perspectives do not presuppose Westphalian territoriality, such approaches could contribute valuably to understanding less understood cases of strategic actors who lack conventional nation-state attributes and capabilities (such as the EU and Big Tech companies). However, their insights also extend beyond these cases. Critical and constructivist approaches to geopolitics have also been fruitfully applied to analyze and explain the behaviour of nation state actors (see for example Branch, 2020; Weldes, 1999; Ruggie, 1993).

Three critical gaps in the literature addressed by the thesis

Drawing from these approaches exposes three specific gaps about the emergence, drivers, and characteristics of geostrategic competition in and through cyberspace, as follows:

1) The EU's emergence as a geostrategic actor in and through cyberspace, including the Union's expression of 'digital sovereignty' claims and their consequences for the EU's development as a global cyber actor;
2) The conceptual basis of 'cyber capabilities' and how they relate to the capacity to engage in geostrategic competition in and through cyberspace;
3) The ontological security and/or 'irrational' bases of geostrategic behaviour in and through cyberspace.

As Chapter 1 laid out, these areas of research will be examined in the form of three research articles (Chapters 4-6). Below, I briefly elaborate these lacunae and position them within the

scholarship reviewed in this chapter. However, Chapters 4-6 will explain the research gaps and their contributions to the field in further detail.[31]

Gap 1: The EU's emergence as a geostrategic actor and its engagement with sovereigntist practices[32]

Neither mainstream IR scholarship nor EU Studies have deeply examined the European Union's geostrategic approach to cyberspace. In fact, as I noted earlier in the chapter, the EU's emergence as a geostrategic cyber actor was largely surprising for dominant IR accounts and for EU studies literature. Meanwhile, for EU studies scholars, 'Neither its history nor its unique institutional structure suggested that the EU would be well positioned for this geoeconomic turn' (Bauerle Danzmann & Meunier, 2024, p. 1097).[33] Indeed, 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 (Nicolaidis et al., 2015; Zielonka, 2006). 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 century,' (Guzzini, 2012, p. 6, emphasis my own).

Contrary to these expectations, geostrategic concepts have become explicitly legitimized under the contemporary European 'geopolitical Commission' (Haroche, 2022).

This is a significant gap in our knowledge. Not only is the EU widely considered to be a powerful global market and normative actor (Bradford, 2020; Manners, 2002), but it

[31] The reader may refer themselves to these chapters 4-6 for further reading.
[32] Refer to Chapters 5 and 6 for further discussion on this topic.
[33] When Bauerle Danzmann and Meunier use the term 'geoeconomic', they mean 'put[ing] economic tools at the service of geopolitics' (2024, p. 1098).

has been touted as an emerging 'digital empire' and 'digital hub' (Drezner et al., 2021) with 'extraterritorial' power (Kuner, 2019). Empirical evidence reveals that the EU has advanced its own cyber norms in the cyber domain (Renard, 2018), including towards geopolitically contested areas, such as its Neighbourhood (e.g. Ukraine, Belarus, and other post-Soviet states) and its Asian periphery (European Parliament, 2020).

Critically, EU studies scholarship has only recently applied itself to the EU's geostrategic turn and it has tended to emphasize exogenous/systemic variables and material security concerns (e.g. Sino-American competition and rising global insecurities). Notwithstanding their insights, this has led significant gaps in our knowledge about the immaterial and ideational drivers of this behaviour; the EU's emergence as a *distinctive* geostrategic cyber actor; and the relationship between the EU's sovereigntist discourse and concrete policy changes. Indeed, the bulk of EU cybersecurity studies approaches have focused upon incoherence in the EU's approach to cyberspace, including the Union's institutional and decision-making processes (Carrapico & Barrinha, 2017; Fahey, 2014; Sliwinski, 2014).[34] However, the field has scarcely explored how the Union's digital sovereignty discourse comes to bear upon actual policy changes towards spatial control in and through cyberspace.

By examining this lacuna, this research offers an important contribution to cyber politics and IR literature, which has not yet examined the EU's development or its ambitions to become a distinctive 'sovereign' actor in the cyber domain in depth. Undertaking further research on this topic would not only extend knowledge beyond the cases of traditional 'great power' activity in the cyber domain, but it would also provide the means for further challenging realist and state-centric assumptions about geopolitical competition and the

[34] Such work echoes criticisms of the EU's activities in other foreign policy areas, such as its external relations with Third Countries (Carbone, 2011; Diez, 2013; Juncos, 2016; Pomorska & Vanhoonacker, 2016). Problematically, these arguments have tended to evaluate the EU's policymaking process against the state as the 'standard', despite the fact that the EU's security and foreign policy process elides a supranational-intergovernmental dichotomy (Bickerton, 2011).

exercise of cyber power in cyberspace. With regards to EU studies, this research would also help to address an important (cyber-specific) gap in studies of EU foreign policy, particularly as it relates to the question of geopolitics and what this tells us about the EU's (aspiring) identity as a global actor. To this end, my project engages directly with ideational approaches to EU foreign policy and extends them to the cyber domain.

Gap 2: The conceptual basis of 'cyber capabilities' and how they relate to the capacity to engage in geostrategic competition in and through cyberspace[35]

Second, the bulk of mainstream IR approaches to geostrategic competition emphasize the significance of 'cyber capabilities' for shaping dynamics of competition and behaviour.[36] Notwithstanding its contributions, this approach has conceptual and empirical limitations, leading to a limited understanding of geostrategic competition in and through cyberspace. First, as I have already explained in this chapter, cyber capabilities are difficult to operationalize, and they cannot adequately explain the emergence or the consequences of geostrategic behaviour practiced by weaker and/or traditionally incapable actors, such as the EU. These tensions have yielded a theoretically 'fuzzy' understanding of cyber power (as capabilities) and its relationship to geostrategic competition.

Notably, the precise meaning of cyber capabilities and its relationship to an actor's capacity to engage in geostrategic behaviour in and through cyberspace remains undertheorized. Are cyber capabilities equal to a resource, as in 'cyber weapons'—comprising the 'propagation method, payload, and exploits' (Stevens, 2018, p. 487)—or are they referring to an *exercise* concept of power? Mainstream scholarship has adopted both meanings, whereby the 'capability' to act in and through cyberspace has often been linked

[35] Refer to Chapter 4 and Chapter 5 for a further discussion of this topic.
[36] Notably exceptions include Betz & Stevens (2011) and Dunn Cavelty & Wenger (2022).

to the *exercise* of material particular capabilities and/or strength.[37] This is also reflected in practice. For example, the Tallinn Manual 2.0 defines 'cyber espionage' as 'any act undertaken clandestinely or under false pretences that *uses* cyber capabilities to gather, or attempt to gather, information' (2017, p. 168, emphasis my own), but 'cyber espionage' also includes '*the capability to* monitor activities in their new destination and report back on them [exfiltration]' (2017, p. 173, emphasis my own). Similarly, the United States defines a 'cyber capabilities' as 'a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.'[38]

Theoretically, the concept of 'cyber capacity' for geostrategic competition has often been equivocated and/or conflated with capabilities in IR scholarship (see for example Kostyuk, 2021; 2024).[39] Assumptions about what capacity in cyberspace might entail have included the deployment of cyber operations for subversion, largely between powerful state adversaries (especially the Russian, American, and Chinese contexts; see Maschmeyer, 2023; Chesney & Smeets, 2023). For example, Maschmeyer's (2023) evaluation about the strategic value of cyber operations as subversive tools is premised upon the significance of state capacity.[40] Separately, Slayton's (2016) critique of ODB theory, discussed earlier in the chapter, rests on the premise that human capacity—not only technological and geographic variables—is an important aspect of achieving both cyber offence and defence objectives.

---

[37] This is also the case for IR theories beyond cyberspace, notably by realist and English School scholars (see for example Keene, 2014, p. 653).

[38] *U.S. Code § 398a - Pilot program for sharing cyber capabilities and related information with foreign operational partners*. Accessible here: https://www.law.cornell.edu/uscode/text/10/398a#g2.

[39] However, it should be noted that not all realist accounts conflate capabilities with *capacity*. Fareed Zakaria draws from the insights of state building literature to conceptualize state power through a capacity-based framework, arguing that 'capabilities shape intentions…[but] state structure limits the availability of national power' and 'the ease with which central [government] decision makers achieve their ends' (p. 9). Distinct from my account of capacity, Zakaria positions his account firmly within a realist, materialist, and state-centric logic, conceiving of states as 'billiard balls […] made of a different *material*, affecting [their] speed, spin, and bounce on the international plane,' (p 1998, p. 9).

[40] As Maschmeyer argues, while erosion is the strategy most suitable for cyber operations, it faces two key limitations: significant organization capacity and resources (thus reserving it for 'stronger' or 'great power' actors) and operational challenges which arise during their deployment (2023, p. 588).

At present, however, the literature lacks a clear framework on the distinction (if any) between 'cyber capabilities' and 'cyber capacity'.

These conceptual ambiguities have produced significant theoretical and empirical blind spots. Empirically, the literature has scarcely explained or discussed the implications of (cyber) capacity building programmes in and through cyberspace, which have acquired greater strategic importance as a foreign policy tool, as I explain in Chapter 4. The wider literature on capacity building has recently recognized that external capacity building assistance schemes now rest at the nexus of security, foreign policy, and development (Collett & Barmpaliou, 2021), but it has failed to explore the possible geopolitical dimension to such practices. While these programmes and tools have been scarcely examined by scholarship, geopolitical competition between powerful actors could play a significant part in capacity building investment decisions—beyond the transfer and/or deployment of certain 'cyber weapons' (in fact, transferring cyber capabilities is very uncommon). Currently, we lack an adequate understanding about the meaning of 'cyber capacity' as a (geo)strategic tool of competition, and the broader strategic significance of capacity building within actors' foreign policy agendas.

Theoretically, it is unclear whether 'cyber capabilities' as it is conceptualized by mainstream approaches to cyber geopolitics accurately accounts for the scope and agentic dimensions of *cyber capacity* to act (geostrategically) in and through cyberspace. There are three relevant bodies of literature which could serve as valuable points of departure for developing a clearer understanding of the capacity to project power in and through cyberspace. First, outside of specific debates about cyber-geostrategic competition, classical 'state-society' approaches to capacity in political science often draw upon Michael Mann's concept of infrastructural power, 'or the [domestic] capacity of the state to penetrate society and "to implement logistically political decisions throughout the realm",' (Mann, 1994, p.

189, quoted in Hanson & Sigman, 2021). A Mannian concept of infrastructural power encompasses the state's *capabilities* (defined as resources), its *effects on society*, and its *territoriality* (Hanson & Sigman, 2021). Similarly, Cingolani argues that there are three manifestations of infrastructural power: 'state *endowments* (which includes financial and bureaucratic resources), state spatial *reach,* and state *legitimacy*,' (2023, p. 278). This scholarship thus advances an understanding of 'capacity' in a broader sense than pure capabilities, including infrastructural dimensions, the significance of political legitimacy, as well as the significance of spatial control and territoriality.

Second, EU Studies on actorness have conceptualized 'capacity' from an agentic perspective, in terms of the EU's capacity to imagine and realize roles for its 'self' in (specific contexts of) international affairs,' derived from 'the interplay of (domestic and external) role expectations, creative action and (social and material) resources,' (Klose, 2018, p. 1146). This provides a fruitful basis for approaching capacity from an agentic perspective, thereby exploring the relationship between imaginaries of the Self, the structural aspects of cyberspace, and the relational aspects of global geopolitical competition. However, this literature has yet to explore the case of the EU's development as a geopolitical cyber actor.

Third, critical and constructivist scholarship suggests that the capacity to achieve strategic goals is shaped by elite perceptions, existential anxieties / ontological security drives, and the institutional context. By emphasizing the agentic and socially constructed dimension to notions of capacity, this conception of capacity is distinct from realist approaches to the concept.[41] For example, perceptions about the provenance of cyber

[41] See for example Kostyuk, 2021; 2023. However, not all realist accounts conflate capabilities with *capacity*. Fareed Zakaria draws from the insights of state building literature to conceptualize state power through a capacity-based framework, arguing that 'capabilities shape intentions…[but] state structure limits the availability of national power' and 'the ease with which central [government] decision makers achieve their ends' (p. 9). Distinct from my account of capacity, Zakaria positions his account firmly within a realist,

capabilities and notions of cyber (in)capacity may be underpinned by particular—and not necessarily rational—imaginaries of the future threat environment (Eberle & Daniel, 2022). As Jordan Branch explained in the context of American offensive cyber operations,

> 'Although threats or attacks on hardware create pressure for a policy response—and the US operation was itself a reaction to Russian interference—the form of that response is underdetermined by material or strategic circumstances and thus is also shaped by ideational factors, including the effects of language itself,' (2021, p. 40).

In this way, the design and decision to use particular material capabilities are shaped by notions of the capacity to act in a given political context, which in turn are influenced by ideational factors. The next section elaborates further on the potential relationship between ontological security and capacity-building approaches by cyber actors.

Overall, the insights of this scholarship complicate materialist approaches to the (objective) strategic import of particular cyber capabilities and their link to geostrategic competition. Given that cyber capabilities are hard to observe and operationalize *and* their strategic purpose is often hard to distinguish, theorizing how various notions of cyber capacity interact with the exercise of cyber capabilities would advance our understanding about cyber power and strategic behaviour. Plausibly, the analytical concept of capacity could be valuable for understanding the behaviour of actors who lack the quintessential 'cyber capabilities' yet have nevertheless pursued ambitious geopolitical and sovereigntist goals towards cyberspace (namely, the EU). Additionally, it would open up further theoretical and empirical scrutiny towards 'capacity building' as a concept for developing and projecting power in and through cyberspace, including in the context of geostrategic competition.

---

materialist, and state-centric logic, conceiving of states as 'billiard balls […] made of a different *material*, affecting [their] speed, spin, and bounce on the international plane,' (p 1998, p. 9).

Gap 3: Ontological insecurity and geostrategic competition[42]

Third, cyber-IR scholarship has long recognized that there is a puzzling—or at least *challenging*—ontological dimension to cyber-IR, including in the EU policy context. Elsewhere, ontological security conditions are theorized to underpin an actor's agency and sense of existence in the world—that is, their capacity to act in time and space, in relation to others (Krickel-Choi, 2024; Mitzen, 2018). For example, ontological security drives have been theorized to condition states' foreign policy behaviour (Subotić, 2016), including their engagement with geopolitical and/or spatial concepts (Eberle & Daniel, 2022).

However, as reviewed in this chapter, mainstream literature and critical scholarship alike has scarcely interrogated the ontological security implications of this for actors and the consequences for geopolitical behaviour. Yet—strikingly—cyber-IR scholarship has *equivocated* this possibility, insofar as it has widely emphasized how cyberspace has created ontological uncertainties for both policymakers and scholars alike, having consequences for strategic decision making. Significantly, Lucas Kello (2017) highlighted one 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, leading to 'unpeace'. Similarly, Maria Mälksoo argued 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,' (emphasis my own, 2018, p. 378). Critical security studies approaches, reviewed in the previous section, further highlight the increasing institutional, political and strategic complexity of cybersecurity issues. Uncertainty about what to 'expect' from others in one's surrounding environment, or distrust in others' behavioural consistency, is illustrated by enduring attribution problems in cyberspace, the

[42] Refer to Chapter 6 for an in-depth review of this gap.

significance of cyber operations for ‘gray zone’ operations, and ongoing debates about how the US’ strategy of persistent engagement could be perceived as escalatory (Dunn Cavelty & Wenger, 2022). Conceivably, these uncertainties could generate ontological security seeking behaviour (see also Lupovici, 2023).

Contributions in critical security studies scholarship have demonstrated that strategic decisions follow ‘logics of appropriateness’ cogent to the particular frames of thinking and metaphorical associations they attribute to certain policy issues (see for example Weldes, 1999). For example, Branch argues in the context of United States foreign policy that the cyberspace-domain rhetorical conjunction has opened possibilities for constructing the internet as ‘a virtual space with territorial features, within which military ideas, strategies, goals, and actions apply,’ (2021, p. 56). By this account, territorial goals and rationales may be transposed onto cyberspace, albeit for potentially irrational reasons (Branch, 2024; see also Eberle & Daniel, 2022; see also Betz & Stevens, 2013).

However, despite recognizing the complex ontological challenges inherent to strategizing in cyberspace (e.g. Lupovici, 2022; Gomez & Whyte, 2021), ontological security studies literature has not comprehensively explored the relationship between strategic uncertainty and rise of geopolitical and sovereignty discourses. Moreover, 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.

Drawing upon the insights of ideational scholarship reviewed above, an analytical focus upon the ‘ontological dimension’ to cyber policymaking foregrounds the under-explored nexus between how policymakers negotiate ontological challenges vis-a-vis cyberspace and their development of particular discourses and strategies. Accordingly, this approach also has the tools to capture EU policymaking dynamics which have elided realist

and state-centric paradigms, (which have generally taken this dynamic for granted). Scholars have demonstrated that the EU has struggled to conceptualize cyberspace as a strategic domain (Carrapico & Farrand, 2017), suggesting that EU policymakers indeed experience ontological challenges. Indeed, 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 (Mitzen, 2018). 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. Beyond the EU, exploring this gap has the potential to broaden our general understanding about the relationship between ontological security drives in and through cyberspace and geostrategic behaviour in this context.

Chapter summary

This chapter adopted a critical ontological approach to argue that mainstream IR literature's state-centric and capabilities-based approach to geostrategic competition in and through cyberspace has left several important gaps in our understanding of the emergence, drivers, and characteristics of this phenomenon. Critically, it has circumscribed our understanding of the EU's development as a geopolitical actor in and through cyberspace and undertheorized the concept of 'cyber capacity' and the potential relationship between ontological security drives and geostrategic behaviour. In the next chapter, I lay out the broad analytical and methodological approach undertaken by this integrated thesis and provide further empirical context on the EU's emergence as a geostrategic actor in and through cyberspace.

Chapter 2 References

Acheson, D. (1969). *Present at the creation: My years in the State Department* (p. 405). Norton.

Agnew, J. (1994). The territorial trap: The geographical assumptions of international relations. *Review of International Political Economy, 1*(1), 53–80.

Agnew, J. & Corbridge, S. (1989) The new geopolitics: The dynamics of geopolitical disorder. In R J. Johnston and P. J. Taylor (eds) *A World in Crisis?: Geographical Perspectives*. Oxford: Blackwell, 266–288.

Ajili, H., & Rouhi, M. (2019). Iran's military strategy. *Survival, 61*(6), 139–152. https://doi.org/10.1080/00396338.2019.1688575.

Anghie, A. (2005). *Imperialism, Sovereignty and the Making of International Law.* Cambridge: Cambridge University Press.

Arquilla, J., & Ronfeldt, D. (Eds.). (2001). *Networks and netwars: The future of terror, crime, and militancy.* RAND National Security Research Division. https://www.rand.org/pubs/monograph_reports/MR1382.html/

Baezner, M., & Cordey, S. (2022). Influence operations and other conflict trends. In M. Dunn Cavelty & A. Wenger (Eds.), *Cyber security politics: Socio-technological transformations and political fragmentation* (1st ed., pp. 17–31). Routledge.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security, 1*(2), 176–198. https://doi.org/10.1017/eis.2016.8.

Balzacq, T., Léonard, S., & Ruzicka, J. (2015). 'Securitization' revisited: Theory and cases. *International Relations, 30(*4), 494–531. https://doi.org/10.1177/0047117815596590.

Barder, A. D. (2019). Social constructivism and actor-network theory: Bridging the divide. In *Tactical constructivism, method, and international relations* (1st ed., p. 13). Routledge.

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *Electronic Frontier Foundation*. https://www.eff.org/cyberspace-independence.

Barkawi, T. (2016). Decolonising war. *European Journal of International Security*, 1(2), 199–214. doi:10.1017/eis.2016.7.

Barrinha, A., & Christou, G. (2022). Speaking sovereignty: The EU in the cyber domain. *European Security, 31*(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895.

Bauerle Danzman, S., & Meunier, S. (2024). The EU's geoeconomic turn: From policy

laggard to institutional innovator. *Journal of Common Market Studies, 62*, 1097–1115. https://doi.org/10.1111/jcms.13599.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security, 31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887.

Bennett, M. M., & Eiterjord, T. (2022). Remote control? Chinese satellite infrastructure in and above the Arctic global commons. *The Geographical Journal*, *188*(4), 1–14. https://doi.org/10.1111/geoj.12503.

Berenskoetter, F. (2017). Approaches to Concept Analysis. *Millennium: Journal of International Studies, 45*(2), 151-173. https://doi.org/10.1177/0305829816651934.

Betz, D., Stevens, T. (2011). *Cyberspace and the state: toward a strategy for cyber-power.* Routledge.

Bickerton, C. J. (2011). Towards a social theory of EU foreign and security policy. *Journal of Common Market Studies, 49*(1), 171–190. https://doi.org/10.1111/j.1468-5965.2010.02138.x.

Blagden, D. (2021). When does competition become conflict? Technology, geography, and the offense–defense balance. *Journal of Global Security Studies, 6*(4), Article ogab007. https://doi.org/10.1093/jogss/ogab007.

Boulding, K. E. (1962). *Conflict and defense: A general theory*. Harper and Brothers.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Cambridge, MA: Harvard University Press.

Bradford, A. (2020). *The Brussels effect: How the European Union Rules the World.* Columbia Law School.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization, 7*5(1), 39–70. doi:10.1017/S002081832000051X

Branch, J. (2024). Territory, sovereignty, and boundaries in digital battlespace. In T. Stevens & J. Devanny (Eds.), In *Research Handbook on Cyberwarfare* (pp. 301–315). Cheltenham, UK: Edward Elgar Publishing.

Broeders, D., Adamson, L., & Creemers, R. (2019). *Coalition of the unwilling? Chinese and Russian perspectives on cyberspace* (The Hague Program for Cyber Norms Policy Brief). SSRN. https://ssrn.com/abstract=3493600.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative Power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies, 61*(5), 1261–1280.

Broeders, D., Sukumar, A., Kello, M., & Andersen, L. H. (2025). Digital corporate

autonomy: geo-economics and corporate agency in conflict and competition. *Review of International Political Economy*, 1–25. https://doi.org/10.1080/09692290.2025.2468308

Bueger, C., Liebetrau, T., & Franken, J. (2022). *Security threats to undersea communications cables and infrastructure – consequences for the EU* (Policy Department for External Relations, European Parliament Report No. EP/EXPO/SEDE/FWC/2019-01/LOT4/1/C/12). European Parliament. https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Buzan, B., & Wæver, O. (2003). Regions and powers: The structure of international security. Cambridge University Press.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis.* Lynne Rienner Publishers.

Cadier, D. (2019). The geopoliticisation of the EU's Eastern Partnership. *Geopolitics, 24*(1), 71–99. https://doi.org/10.1080/14650045.2018.1477754.

Cai, C. (2018). Geopolitics in the cyberspace: A new perspective on U.S.-China relations. *The Journal of International Studies, 39*(1). http://jtp.cnki.net/bilingual/detail/html/GJZY201801001?view=3

Carbone, M. (2011). The European Union and China's rise in Africa: Competing visions, coherence and trilateral cooperation. *Journal of Contemporary African Studies*, 29(2), 203–221. https://doi.org/10.1080/02589001.2011.555195.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber)security actor? *Journal of Common Market Studies, 55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575

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

Chander, A., & Sun, H. (2021). *Sovereignty 2.0* (Georgetown Law Faculty Publications and Other Works No. 2404; University of Hong Kong Faculty of Law Research Paper No. 2021/041). https://doi.org/10.2139/ssrn.3904949.

Chesney, R., & Smeets, M. (Eds.). (2023). *Deter, disrupt, or deceive: Assessing cyber conflict as an intelligence contest*. Georgetown University Press.

Choucri, N. & Clark, D. D. (2012). Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. *In Explorations in Cyber-International Relations: Who Controls Cyberspace?* Cambridge: MIT Press.

Choucri, N., & Clark, D. D. (2018). The Cyber-IR System: Integrating Cyberspace and International Relations. In *International Relations in the Cyber Age: The Co-Evolution Dilemma* (pp. 101–121). MIT Press.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Palgrave Macmillan.

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

Cingolani, L. (2023). Infrastructural state capacity in the digital age: What drives the performance of COVID-19 tracing apps? *Governance, 36*(1), 275–297. https://doi.org/10.1111/gove.12666.

Clark, J.A., and A Jones. 2011. "The Spatialising Politics of European Political Practice: Transacting 'Eastness' in the European Union." *Environment and Planning D: Society and Space* 29(2): 291–308.

Council of the European Union. (2015). Council conclusions on cyber diplomacy [6122/15].

Costa, O., & Barbé, E. (2023). A moving target: EU actorness and the Russian invasion of Ukraine. *Journal of European Integration, 45*(3), 431–446. https://doi.org/10.1080/07036337.2023.2183394.

Craig, A. J. S., & Valeriano, B. (2018). Realism and cyber conflict: Security in the digital age. In D. Orsi, J. R. Avgustin, & M. Nurnus (Eds.), Realism in practice: An appraisal (pp. 85–101). *E-International Relations.*

Creemers, Rogier. (2024). The Chinese Conception of cybersecurity: A conceptual, institutional, and regulatory genealogy. Journal of Contemporary China, 33(146), 173–188. http://dx.doi.org/10.1080/10670564.2023.2196508

Cristiano, F., Kurowska, X., Stevens, T., Hurel, L. M., Fouad, N. S., Cavelty, M. D., … Shires, J. (2023). Cybersecurity and the politics of knowledge production: towards a reflexive practice. *Journal of Cyber Policy*, 8(3), 331–364. https://doi.org/10.1080/23738871.2023.2287687

Cruz Lobato, L., & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional, 58*(2), 23–43. https://doi.org/10.1590/0034-7329201500202.

Deudney, D. (2020). Geography, geopolitics, and geohistory. In *Dark skies: Space expansionism, planetary geopolitics, and the ends of humanity* (Chap. 8). Oxford University Press. https://doi.org/10.1093/oso/9780190903343.003.0008

Diez, T. (2013). Normative power as hegemony. *Cooperation and Conflict, 48*(2), 194–210. https://doi.org/10.1177/0010836713485386.

Dodds, K., & Woon, C. (2020, April 30). Classical Geopolitics Revisited. *Oxford Research Encyclopedia of International Studies.* https://oxfordre.com/internationalstudies/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-379.

Douzet, F. (2014). Understanding Cyberspace With Geopolitics. *Hérodote*, No 152-153(1), 3-21. https://shs.cairn.info/journal-herodote-2014-1-page-3?lang=en.

Dunn Cavelty, M., & Egloff, F. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review, 15*(1), 37–57.

Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Dunn Cavelty, M. (2023, October 27). *Cybersecurity research: Unde venis? (An insider's perspective)* [Conference presentation]. The Political Economy of Cyber Conflict Conference, ETH Zürich.

Drezner, D. W., Farrell, H., & Newman, A. L. (2021). *The uses and abuses of weaponized interdependence.* Brookings Institution Press.

Eberle, J., & Daniel, J. (2022). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. *Political Geography, 92*, 102502. https://doi.org/10.1016/j.polgeo.2021.102502.

e-Estonia. (n.d.). e-Governance: Data embassy. Retrieved July 11, 2025, from https://e-estonia.com/solutions/e-governance/data-embassy/.

Eudaily, S. P., & Smith, S. (2008). Sovereign geopolitics? – Uncovering the "sovereignty paradox". *Geopolitics, 13*(2), 309–334. https://doi.org/10.1080/14650040801991621.

European Commission. (2019, November 27). Speech by President-Elect von der Leyen in the European Parliament plenary on the occasion of the presentation of her college of commissioners and their programme.

European Commission. (2021, March 9). *Europe's digital decade: Commission sets the course towards a digitally empowered Europe by 2030*. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983.

European Commission. (2022). Roadmap on critical technologies for security and defence [COM(2022) 61 final].

Fahey, E. (2014.) *The EU's Cybercrime and Cyber-Security Rule-Making: Mapping the Internal and External Dimensions of EU Security*. Amsterdam.

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty – Rhetoric and reality. *Journal of European Public Policy, 31*(8), 2099–2120. https://doi.org/10.1080/13501763.2024.2358984

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy, and sovereignty. *International Affairs, 100*(6), 2379–2397. https://doi.org/10.1093/ia/iiaa156.

Fearon, J. D. (2018). Cooperation, conflict, and the costs of anarchy. *International Organization, 72*(3), 523–559. https://doi.org/10.1017/S0020818318000309.

Fischerkeller, M. P., & Harknett, R. J. (2019). Persistent Engagement, Agreed Competition,
and Cyberspace Interaction Dynamics and Escalation. *The Cyber Defense Rev*iew, 267–287. https://www.jstor.org/stable/26846132.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology, 33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Foulon, M., & Meibauer, G. (2020). Realist avenues to global International Relations. *European Journal of International Relations,* 26(4), 1203–1229. https://doi.org/10.1177/1354066120926706.

Fossum, J. E. (2006). Conceptualizing the European Union through four strategies of comparison. *Comparative European Politics, 4*(1), 94–123. https://doi.org/10.1057/palgrave.cep.6110077.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security, 38*(2), 42–78. https://doi.org/10.1162/ISEC_a_00136.

General Secretariat of the Council. (2022). A strategic compass for security and defence [7371/22].

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. Review of *International Political Economy, 3*0(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Gomez, M. A., & Whyte, C. (2021). Breaking the myth of cyber doom: Securitization and normalization of novel threats. *International Studies Quarterly, 65*(4), 1137–1150. https://doi.org/10.1093/isq/sqab034.

Gravier, M. (2011). Empire vs federation: which path for Europe? *Journal of Political Power,* 4(3), 413–431. https://doi.org/10.1080/2158379X.2011.628854.

Guzzini, S. (2012). *The return of geopolitics in Europe?: Social mechanisms and foreign policy identity crises.* Cambridge University Press.

Guzzini, S. (2013). The ends of International Relations theory: Stages of reflexivity and modes of theorizing. *European Journal of International Relations, 19*(3), 521-541. https://doi.org/10.1177/1354066113494327.

Harknett, R. J., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies, 45*(4), 534–567. https://doi.org/10.1080/01402390.2020.1732354.

Haroche, P. (2023). A 'Geopolitical Commission': Supranationalism meets global power

competition. *JCMS: Journal of Common Market Studies, 61*(4), 970–987. https://doi.org/10.1111/jcms.13440.

Hansen, L., & Nissenbaum, H. F. (2009). Digital disaster, cybersecurity, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155–1175. https://ssrn.com/abstract=2567410.

Hanson, J. K., & Sigman, R. (2021). Leviathan's latent dimensions: Measuring state capacity for comparative political research. *The Journal of Politics, 83*(4), 1495–1510. https://doi.org/10.1086/715163.

Hay, C. (2011). Political ontology. In R. E. Goodin (Ed.), *The Oxford handbook of political science*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199604456.013.0023

Hill, C. (1993). The capability-expectations gap, or conceptualizing Europe's international role. *Journal of Common Market Studies, 31*(3), 305–328. https://doi.org/10.1111/j.1468-5965.1993.tb00466.x

Hix, S. (1994). The study of the European community: The challenge to comparative politics. *West European Politics*, 17(1), 1–30. https://doi.org/10.1080/01402389408424999

Hoffmann, S. (1996). Obstinate or Obsolete ? The Fate of the Nation-State and the Case of Western Europe. *Daedalus 95*(3): 862–915.

Howorth, J., & Menon, A. (2009). Still not pushing back: Why the European Union is not balancing the United States. *Journal of Conflict Resolution, 53*(5), 727–744. https://doi.org/10.1177/0022002709339362.

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics, 30*(2), 167–214.

Joint Chiefs of Staff. (2018, June 8). *Joint publication 3-12: Cyberspace operations*. https://nsarchive2.gwu.edu/dc.html?doc=4560063-Joint-Chiefs-of-Staff-Joint-Publication-3-12

Kadercan, B. (2015). Triangulating territory: A case for pragmatic interaction between political science, political geography, and critical IR. *International Theory, 7*(1), 125–161. https://doi.org/10.1017/S1752971914000402

Kaminska, M. (2021). Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. *Journal of Cybersecurity, 7*(1), Article tyab008. https://doi.org/10.1093/cybsec/tyab008.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security, 38*(2), 7–40. http://www.jstor.org/stable/24480929

Kello, L. (2017). *The Virtual Weapon and International Order.* Yale University Press.

Kello, L. (2022). *Striking back: The end of peace in cyberspace—and how to restore it*.

Yale University Press.

Keene, E. (2014). The Standard of 'Civilisation', the Expansion Thesis and the 19th-century International Social Space. *Millennium, 42(*3), 651-673. https://doi.org/10.1177/0305829814541319.

Kissinger, H. (1979). *The White House years*. Little, Brown.

Khong, Y. F. (2019). Power as prestige in world politics. International Affairs, 95(1), 119–142. https://doi.org/10.1093/ia/iiy245

Klimburg, A., & Tirmaa-Klaar, H. (2011). *Cybersecurity and cyberpower: Concepts, conditions, and capabilities for cooperation for action within the EU*. Directorate-General for External Policies of the Union, Directorate B, Policy Department. https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf

Klose, S. (2020). Interactionist role theory meets ontological security studies: an exploration of synergies between socio-psychological approaches to the study of international relations. *European Journal of International Relations,* 26(3), 851-874. https://doi.org/10.1177/1354066119889401.

Klose, S. (2018). Theorizing the EU's actorness: Towards an interactionist role theory framework. *JCMS: Journal of Common Market Studies, 56*, 1144–1160. https://doi.org/10.1111/jcms.12725.

Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty*. Oxford University Press.

Kostyuk, N., & Gartzke, E. (2022). Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine. *Texas National Security Review*, 5(3), 113–126. http://dx.doi.org/10.26153/tsw/42073.

Kostyuk, N. (2024). Allies and diffusion of state military cybercapacity. *Journal of Peace Research,* 61(1), 44-58. https://doi.org/10.1177/00223433241226559.

Kostyuk, N. (2021). Deterrence in the cyber realm: Public versus private cyber capability. *International Studies Quarterly 65*(4): 1151–1162.

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.

Krickel-Choi, N. C. (2021). *The embodied state: Why and how physical security matters for ontological security. Journal of International Relations and Development*, 25(1), 159–181. https://doi.org/10.1057/s41268-021-00219-x.

Kuner, C. (2019). The internet and the global reach of EU law. In M. Cremona & J. Scott (Eds.), EU law beyond EU borders: The extraterritorial reach of EU law (pp. 112–145). Oxford University Press.

Kuus, M. (2014.) *Geopolitics and Expertise: Knowledge and Authority in European Diplomacy*. Chichester, West Sussex; Malden: Wiley-Blackwell.

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review*, *22*(3), 482–506. https://doi.org/10.1093/isr/viz022.

Lambach, D. (2024). B/ordering the state in cyberspace. In A. Fellner, K. Jungbluth, H. Krämer, & C. Wille (Eds.), *Border studies: Cultures, spaces, orders* (pp. 285-307). Europa-Universität Viadrina Frankfurt.

Latour, B. (1996). On actor-network theory: A few clarifications. *Soziale Welt* 47, pp. 369-381. Accessible here: http://www.bruno-latour.fr/sites/default/files/P-67%20ACTOR-NETWORK.pdf.

Lehdonvirta, V. (2022). *Cloud empires: How digital platforms are overtaking the state and how we can regain control*. The MIT Press.

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025). Weaponised interdependence in a bipolar world: how economic forces and security interests shape the global reach of US and Chinese cloud data centres. *Review of International Political Economy,* 1–26. https://doi.org/10.1080/09692290.2025.2489077.

Lerner, A. B., & O'Loughlin, B. (2023). Strategic ontologies: Narrative and meso-level theorizing in international politics. *International Studies Quarterly, 67*(3), Article sqad058. https://doi.org/10.1093/isq/sqad058.

Lewis, J. A. (2020). Sovereignty and the evolution of Internet ideology. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology.

Liebetrau, T., & Christensen, K. K. (2021). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security,* 6(1), 25–43. doi:10.1017/eis.2020.10.

Lieber, K. (2014). The offense-defense balance and cyber warfare. In E. O. Goldman & J. Arquilla (Eds.), *Cyber analogies* (pp. [96-107]). Naval Postgraduate School. https://core.ac.uk/download/pdf/36732393.pdf.

Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security, 39*(3), 7–47. https://doi.org/10.1162/ISEC_a_00189

Lindsay, J., & Gartzke, E. (2016). Coercion through cyberspace: The stability-instability paradox revisited. In K. M. Greenhill & P. J. P. Krause (Eds.), *The power to hurt: Coercion in theory and in practice*. Oxford University Press.

Lindsay, J. R., & Gartzke, E. (2020). Politics by many other means: The comparative strategic advantages of operational domains. *Journal of Strategic Studies, 45*(2), 746–773. https://doi.org/10.1080/01402390.2020.1768372

Lindsay, J. R. (2022). Quantum computing and classical politics: The ambiguity of advantage in signals intelligence. In M. Dunn Cavelty & A. Wenger (Eds.), *Cyber security politics: Socio-technological transformations and political fragmentation* (1st ed., pp. 80–94). Routledge. https://doi.org/10.4324/9781003110224.

Lonergan, E. D., & Lonergan, S. W. (2023). *Escalation Dynamics in Cyberspace*. Oxford University Press.

Lupovici, A. (2022). Uncertainty and the study of cyber deterrence: The case of Israel's limited reliance on cyber deterrence. In M. Dunn Cavelty & A. Wenger (Eds.), *Cyber security politics: Socio-technological transformations and political fragmentation* (1st ed., pp. 128–137). Routledge. https://doi.org/10.4324/9781003110224.

Lynn-Jones, S. M. (1995). Offence-defence theory and its critics. *Security Studies, 4*(4), 660–691. https://doi.org/10.1080/09636419509347600.

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: The emerging practices of the EU and NATO. *European Security, 27*(3), 374–392. https://doi.org/10.1080/09662839.2018.1497984.

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies, 40*(2), 235–258. https://doi.org/10.1111/1468-5965.00353.

Maschmeyer, L. (2022). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies, 46*(3), 570–594. https://doi.org/10.1080/01402390.2022.2104253.

Maurer, T., & Morgus, R. (2014). *Compilation of existing cybersecurity and information security related definitions*. New America. https://www.jstor.org/stable/resrep10487.5

McCarthy, D. R. (2015). *Power, information technology, and international relations theory: The power and politics of US foreign policy and the internet*. London: Palgrave Macmillan.

Mearsheimer, J. J. (2001). *The tragedy of great power politics.* W. W. Norton & Company.

Mercer, J. (2017). The illusion of international prestige. *International Security, 41*(4), 133–168. https://doi.org/10.1162/ISEC_a_00276

Microsoft. (2025). *Microsoft Cloud for Sovereignty*. https://www.microsoft.com/en-us/industry/sovereignty/cloud.

Moore, D. (2022). *Offensive cyber operations: Understanding intangible warfare*. Oxford University Press.

Monsees, L., Liebetrau, T., Austin, J. L., Leander, A., & Srivastava, S. (2023). Transversal politics of Big Tech. *International Political Sociology, 17*(1), Article olac020. https://doi.org/10.1093/ips/olac020.

Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace* (4th ed.). New York, NY: Alfred A. Knopf.

Mueller, M. (2020). Against sovereignty in cyberspace. *International Studies Review, 22*(4), 779–801. https://doi.org/10.1093/isr/viaa030

Mueller, M. (2010). *Networks and states: The global politics of internet governance*. MIT Press.

NATO. (2024, July 30). *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Nicolaïdis, K., Sebe, B., & Maas, G. (Eds.). (2015). *Echoes of empire: Identity, memory and colonial legacies.* I.B. Tauris.

Nye, J. S., Jr. (2014). *The regime complex for managing global cyber activities* (CIGI Publications No. 1, pp. 1–15*). Centre for International Governance Innovation (CIGI).* https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities/.

Nye, J. (2010). *Cyber power*. Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/cyber-power.

Ó Tuathail, G. (1998). Postmodern geopolitics? The modern geopolitical imagination and beyond. In S. Dalby & G. Ó Tuathail (Eds.), *Rethinking geopolitics* (1st ed., pp. 1 6–38). Routledge. https://doi.org/10.4324/9780203058053.

Pawlak, P. (2018). Operational guidance for the EU's international cooperation on cyber capacity building. European Commission. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf.

Pohle, J., Nanni, R., & Santaniello, M. (2024). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet, 16*(3), 666–671. https://doi.org/10.1002/poi3.437.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the internet and the global digital order. *Policy & Internet,* 14(1), 13–27. https://doi.org/10.1002/poi3.296.

Pomorska, K., & Vanhoonacker, S. (2016). Europe as a global actor: Searching for a new

strategic approach. *Journal of Common Market Studies, 54*(S1), 204–217. https://doi.org/10.1111/jcms.12400.

Raymond, M., & Sherman, J. (2023). Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice. *Contemporary Security Policy, 45*(1), 110–140. https://doi.org/10.1080/13523260.2023.2269809.

Rice, N. F. (2019). Estonia's digital embassies and the concept of sovereignty. *Georgetown Security Studies Review*. https://georgetownsecuritystudiesreview.org/2019/10/10/estonias-digital-embassies-and-the-concept-of-sovereignty/.

Rid, T. (2013). *Cyber War Will Not Take Place.* Hurst Publishers.

Rid, T. (2022, March 18). Why you haven't heard about the secret cyberwar in Ukraine. *The New York Times*. https://www.nytimes.com/2022/03/18/opinion/cyberwar-ukraine-russia.html.

Rühlig, T. (2023). Chinese influence through technical standardization power. *Journal of Contemporary China, 32*(139), 54–72. https://doi.org/10.1080/10670564.2022.2052439

Ruggie, J. G. (1993). Territoriality and beyond: Problematizing modernity in international relations. *International Organization, 47*(1), 139–174. https://www.jstor.org/stable/2706885.

Schimmelfennig, F. (2021). Rebordering Europe: external boundaries and integration in the European Union. *Journal of European Public Policy, 28*(3), 311–330. https://doi.org/10.1080/13501763.2021.1881589.

Schindler, S., Alami, I., DiCarlo, J., Jepson, N., Rolf, S., Bayırbağ, M. K., … Zhao, Y. (2023). The Second Cold War: US-China Competition for Centrality in Infrastructure, Digital, Production, and Finance Networks. *Geopolitics*, 29(4), 1083–1120. https://doi.org/10.1080/14650045.2023.2253432

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations.* Cambridge University Press.

Seidl, T. (2024). Charting the Contours of the Geo-Tech World. *Geopolitics, 29*(5), 2033–2045. https://doi.org/10.1080/14650045.2024.2333358

Simmons, B. A., & Hulvey, R. A. (2023). *Cyberborders: Managing interdependence in the information age*. *Faculty Scholarship at Penn Carey Law*, 3158. https://scholarship.law.upenn.edu/faculty_scholarship/3158.

Sjursen, H. (2011). Not so intergovernmental after all? On democracy and integration in European foreign and security policy. *Journal of European Public Policy, 18*(8), 1089–1105. https://doi.org/10.1080/13501763.2011.615194.

Slayton, R. (2016). What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security,* 41(3), 72–109. https://www.jstor.org/stable/26777791.

Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy, 35*(3), 468–486. https://doi.org/10.1080/13523260.2014.959261.

Sloan, G., & Gray, C. S. (1999). Why geopolitics? *The Journal of Strategic Studies, 22*(2–3), 1–11. https://doi.org/10.1080/01402399908437751.

Smeets, M. (2022). *No shortcuts: Why states struggle to develop a military cyber-force*. Hurst.

Smeets, M. (2025). Ransom war: How cyber crime became a threat to national security. *Hurst Publishing.*

Smeets, M., & Lin, H. S. (2018). Offensive cyber capabilities: To what ends? In *Proceedings of the 10th International Conference on Cyber Conflict (CyCon)*. https://doi.org/10.23919/CYCON.2018.8405010.

Spykman, N. J. (1969). *The geography of the peace* (H. R. Nicholl, Ed.; Illustrated, Reprint ed.). Archon Books.

Stevens, T. (2018). Cyberweapons: power and the governance of the invisible. *International Politics, 55*(3–4), 482–502. https://doi.org/10.1057/s41311-017-0088-y.

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy, 45*(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739

Thomson, J. E. (1995). *State sovereignty in international relations: Bridging the gap between theory and empirical research*. *International Studies Quarterly, 39*(2), 213–233. https://doi.org/10.2307/2600847.

Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). Cybersecurity in the EU common security and defence policy (CSDP): Challenges and risks for the EU (Report no. PE 603.175). *European Parliamentary Research Service.*

Turner, C., & Johnson, D. (2017). Infrastructure and territoriality. In *Global infrastructure networks: The trans-national strategy and policy interface* (pp.1-30). Edward Elgar Publishing.

United Kingdom. (2022). *UK digital strategy*. https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy

United Kingdom. (2022). *National cyber strategy 2022*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

USAID. (2021). *Cybersecurity primer*. https://www.usaid.gov/digital-development/usaid-cybersecurity-primer.

U.S. Cyber Command PAO. (2022, October 25). *CYBER 101 – Defend forward and persistent engagement*. U.S. Cyber Command. https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/.

U.S. Department of Defense. (2001, July 27). *Network centric warfare: Report to Congress*. http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf.

Valeriano, B. (2022). The failure of offense/defense balance in cyber security. *The Cyber Defense Review,* 7(3), 133–146. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/08_Valeriano_CDR_V7N3_Summer_2022.pdf.

Waltz, K. (1979). *Theory of international politics*. Addison-Wesley.

Weaver, D. (2020, June 30). Spatiality and World Politics. Oxford Research Encyclopedia of International Studies. https://doi.org/10.1093/acrefore/9780190846626.013.562.

Weber, V. (2020). *Making sense of technological spheres of influence*. London: LSE IDEAS. Retrieved from https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Technological-Spheres-of-Influence.pdf.

Weber, V. (2018). Linking cyber strategy with grand strategy: the case of the United States. *Journal of Cyber Policy*, 3(2), 236–257. https://doi.org/10.1080/23738871.2018.1511741

Weiler, J. (2020, October 29). Europe must learn quickly to speak the language of power. *EJIL: Talk! Blog of the European Journal of International Law*. https://www.ejiltalk.org/europe-must-learn-quickly-to-speak-the-language-of-power-part-i/.

Weldes, J. (1999). *Constructing national interests : the United States and the Cuban missile crisis* (1st ed.). University of Minnesota Press.

Zakaria, F. (1998). *From Wealth to Power The Unusual Origins of America's World Role*. Princeton University Press.

Zeng, J., T. Stevens, and Y. Chen. 2017. China's solution to global cyber governance: Unpacking the domestic discourse of 'Internet sovereignty'. *Politics & Policy* 45(3): 432–464.

Zekos, G. I. (2013). Demolishing State's Sole Power over Sovereignty and Territory Via Electronic Technology and Cyberspace. Journal of Internet Law 17 (5): 3–17.

Zielonka, J. (2006). *Europe as empire: The nature of the enlarged European Union*. Oxford University Press.

Chapter 3: Background and methodological approach of the integrated thesis

Chapter overview

Given that 'cyber' and 'digital' issues are complex and rapidly evolving issues within the context of European Union external action, this section aims to familiarize the reader with key institutions and actors relevant to this thesis. This contextualizes but does not supplant the empirical analyses in Chapters 4-6.[43] Accordingly, this chapter outlines the scope and orientation of the integrated thesis, including the common methodological, ontological, and epistemological foundations for the dissertation's research articles. It also provides further background on the context of EU cybersecurity policy and its overlap with external action, as well as the timeframe covered by the dissertation.

Background: The European Union as a global cybersecurity actor

While the remit of EU external action has been variably defined by scholars (Keukeleire & Delreux, 2022), it can be understood as 'the area of European policies that is directed at the external environment with the objective of influencing that environment and the behavior of other actors within it, in order to pursue interests, values and goals,' (Keukeleire & Delreux, 2014, p.1). Building on Keukeleire and Delreux (2022), I consider EU external action to encapsulate both the common foreign and security policy, the European security and defence policy, (CSDP/ESDP) and the areas of trade, development, environment, and energy—that is, both the areas of 'external relations' and conventional foreign policy and security. In other words, the EU's global activities can be broadly characterized as 'EU external action.'

[43] For a broader overview of how cyber issues transverse multiple EU policy areas, including beyond the foreign policy context, see Christina Rupp, *Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors*, Interface, June 27, 2024, https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem.

The close relationship between the 'external relations' and classical 'foreign policy' dimensions of the EU's international engagement was formalized with the Lisbon Treaty in 2009, which remains in force today (de Búrca, 2013). While efforts to integrate the EU's 'low politics' external relations policy areas (e.g. trade, aid, and development) with the Union's 'high politics' foreign policy and security mandate were set in motion in the 1990s, the Lisbon Treaty ushered in a new era for the EU's external action (de Búrca, 2013). The Lisbon Treaty mandated the inception of the EU's *European External Action Service* (EEAS), the diplomatic branch of EU global action, and established the High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission (HR/VP). The EEAS and HR/VP role has enabled closer coordination between EU institutions, especially the European Commission's role in external affairs, with the intergovernmental aspects of EU external action (the Council of the EU and Member States' foreign and defence ministries). Thus, the inception of the EEAS and the legalization of the Lisbon treaty preceded the development of the EU's first cybersecurity strategy.

Altogether, the EU's foreign policy and external action remit(s) have changed significantly since its first collective engagement with international relations in the 1950s as a smaller, less integrated political organization (de Búrca, 2013). Outside of cyber-IR scholarship, EU Studies scholars have argued that changes to the EU's global 'actorness'—or the EU's 'capacity to behave actively and deliberately in relation to other actors in the international system' (Sjöstedt, 1977, p. 16)—have been driven by endogenous factors (e.g. developments in European integration) and exogenous factors, including global crises and international security developments (Fawcett, 2015).[44] Not unlike cyberspace, European integration has been characterized as a process of boundary re-definition (Vollaard, 2018),

[44] Currently, the European Parliament (n.d.) describes the EU's 'action on the international scene [as] guided by the principles *that inspired its own creation*, development and enlargement, and which are also embedded in the United Nations Charter and international law.'

whereby territoriality and the EU's functional tasks is atypical to the Westphalian model (Bartolini, 2006). Yet, the EU has not made a full-fledged departure from the nation-state, particularly in terms of where it derives sovereign authority (Fossum, 2006; Bickerton, 2011).

Supranationalism and EU external action post-Lisbon: Broad institutional, political, and legal context

Presently, EU foreign policymaking is characterized by hybridity and supranationalism, it is not reducible to a purely state-centric, intergovernmental conception of foreign policymaking. While the EU's status as a *sui generis* actor is realized by the pooled sovereignty of its Member States (Moravscik, 1998), scholars have established that, following the provisions of the 2009 Lisbon Treaty, *de novo* bodies, namely the European External Action Service (EEAS), and the High Representative/Vice-President of the European Commission (HR/VP), have enjoyed greater power and influence as agenda-setting actors and with greater autonomy from national diplomatic corps in relations with third countries (Balfour et al., 2015; Furness, 2013; Morillas, 2020). [45] Thus, overall, EU external action policy can be understood as a process that is shaped 'with reference to values and principles that are seen as *particular* to the Union,' (Sjursen, 2011, p. 1086).[46]

[45] Including in the context of the EU's 2016 *Global Strategy* (Morillas, 2020).

[46] To be sure, examining EU supranational institutions (viz. the European Commission, the External Action Service, etc.) does not preclude examination of intergovernmental discursive struggles over the meaning of EU digital sovereignty at the horizontal level (e.g. between various Committees and/or Representatives in the Council of the EU) or vertical levels (e.g. between Brussels and Member States). Chapter 5 further details potential drivers and mechanisms of policy change in the EU's external action context. See also Klose, Theorizing the EU's Actorness: Towards an Interactionist Role Theory Framework, JCMS, 2018, p. 1144.

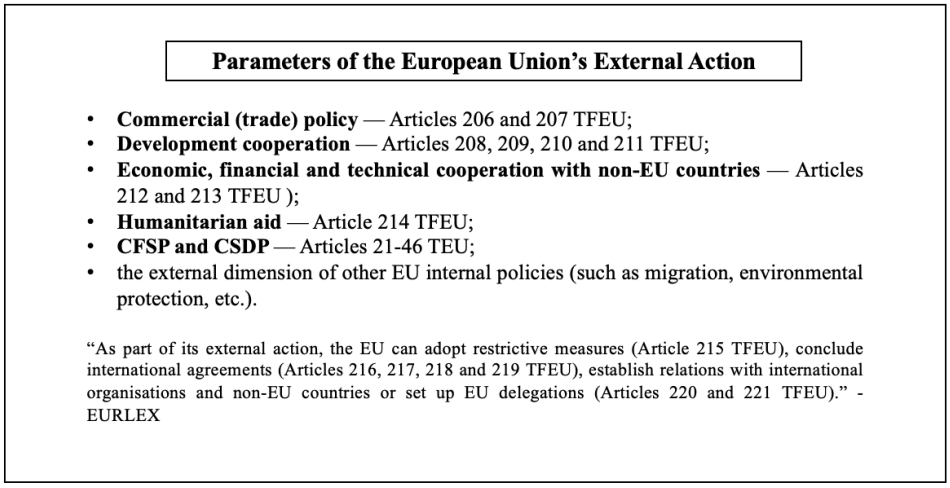


Figure 3.4. Current parameters of the EU's external action, from EURLEX database.

Accordingly, the EU can be considered a non-traditional 'state-based' foreign policy actor. The term '*state-based'* draws attention to the reality that foreign policymaking is situated within particular institutional structures which often (but not always) overlap with the 'state' as a broad field of action (González-Ocantos, 2020).[47] This conceptualization broadly coheres with Bob Jessop's approach to state power, which can be understood to result from 'a continuing interaction between the structurally inscribed strategic selectivities of the state as an institutional ensemble and the changing balance of forces operating within, and at a distance from, the state, and perhaps, also trying to transform it,' (Jessop, 1999; quoted in Moisio & Paasi, 2013, p. 54). State-based power is therefore constituted and reproduced by foreign policymaking practices, as part of the 'process of statecraft' (Kuus, 2009, p. 88; see also Carrapico & Farrand, 2024). Accordingly, state-based power in the context of cyberspace is constituted by the sociotechnical nature of digital technologies and

[47] By 'field of action,' I am loosely drawing upon Bourdieu's conception of a 'field of action' as a social domain which can be understood as a space of action 'with particular morphological and institutional features' (González-Ocantos, 2020, p. 108). As Bourdieu and Wacquant described, the field of action 'guides the strategies whereby occupants of those positions seek, individually or collectively, to safeguard or improve their position in this field. In this sense, the field shapes behaviour yet it also serves as the site of 'struggles aimed at preserving or transforming' the rules (Bourdieu & Wacquant, 1992, p. 101; quoted in González-Ocantos, 2020, p. 109).

their integration into infrastructures relevant to state power, such as critical infrastructure and society (Dunn Cavelty & Wenger, 2022).

EU external action and its intersection with EU cybersecurity policies

Currently, the EU's capacity to act in and through global cyberspace is shaped by varied institutional competences across different areas of external action. For example, in the area of common foreign and security policy (CFSP), sovereignty is pooled between its Member States (Moravscik, 1998), which have been historically hesitant to cede control over their hard security. This arrangement has arguably stunted the Union's 'hard' capabilities (Sliwinski, 2014; Hill, 1993). By contrast, the Commission enjoys exclusive competences over other 'softer' areas of external action: trade and economic security instruments. Generally, EU foreign policy remains characterized by the strong interaction across three institutional pillars of governance (which mandate different degrees of supranational authority) which stem from the 1990s Maastricht-era treaty arrangement (Keukeleire & Delreux, 2022; cf. Smith, 2012).[48]

Notably, the post-Lisbon institutional makeup of EU external action (see Figure 3.4) underscores the influence of EU supranational institutions on EU cyber policy. This level of analysis, scholars have widely argued, captures the bulk of post-Lisbon developments in EU external action aimed at cybersecurity and adjacent digital policies (Trimintzios et al., 2017, p. 5; see also Laurer & Seidl, 2021; Timmers, 2018; Pawlak et al., 2018; Heidebrecht, 2024). As Chapters 4-6 will discuss, the EU has increasingly integrated cybersecurity instruments into its external action outlook, including in the CFSP/ESDP. The basic institutional

[48] Rather than focusing upon the 'pillar' structure, for example, Michael Smith (2022) argued that EU foreign policy has four domains: the market, security and defence, diplomacy, and normative power, although the last dimension has become a subject of much recent debate.

implications of this shift are observable by comparing the EU's first cybersecurity strategy to the contemporary 2020 version, as presented in succession below.

Evolution in EU cyber strategy, 2013-2020

Whereas the EU's 2013 strategy was initially inward-looking and oriented around network information security, the EU's contemporary (2020) cybersecurity strategy encompasses four primary sub policy-areas: cybercrime and law enforcement; critical information infrastructure protection; cyber-defence; and cyber-diplomacy (Carrapico & Farrand, 2024). As can be seen in Figures 3.5 and 3.6 below, the number of institutional actors in EU cyber-foreign policy have proliferated over the last decade, together with an increasingly assertive global outlook. These institutional actors, furthermore, have set up a number of working groups and networks which are not represented in the schematic.[49]

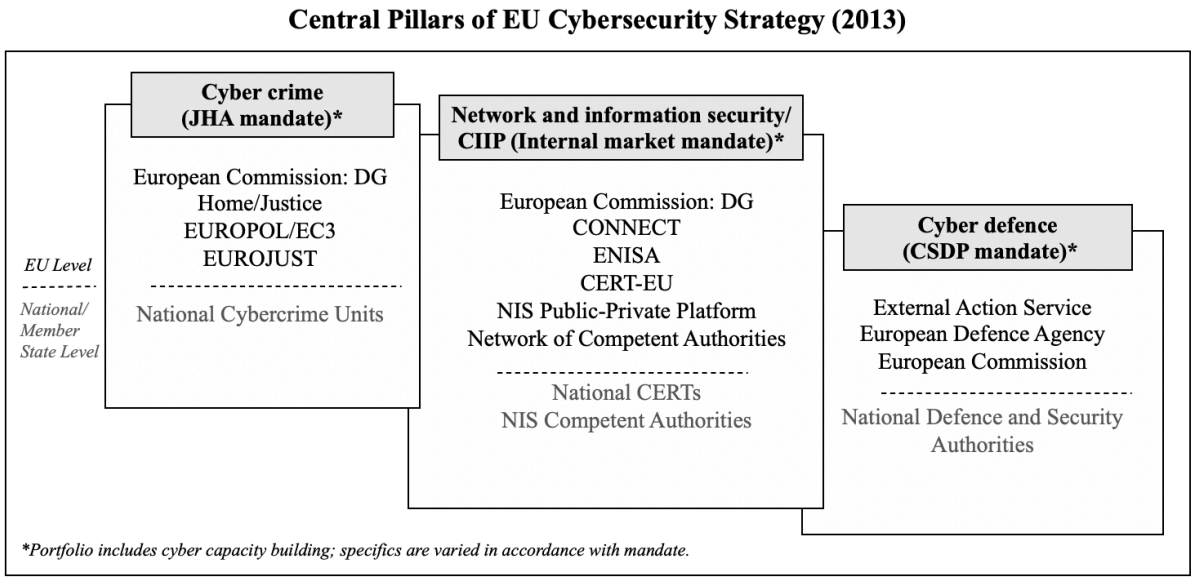


Figure 3.5. Central pillars of EU cybersecurity strategy (2013), as compiled by George Christou. Diagram here was reproduced, with slight modifications, by the author.

[49] They are numerous and beyond the scope of the present discussion.

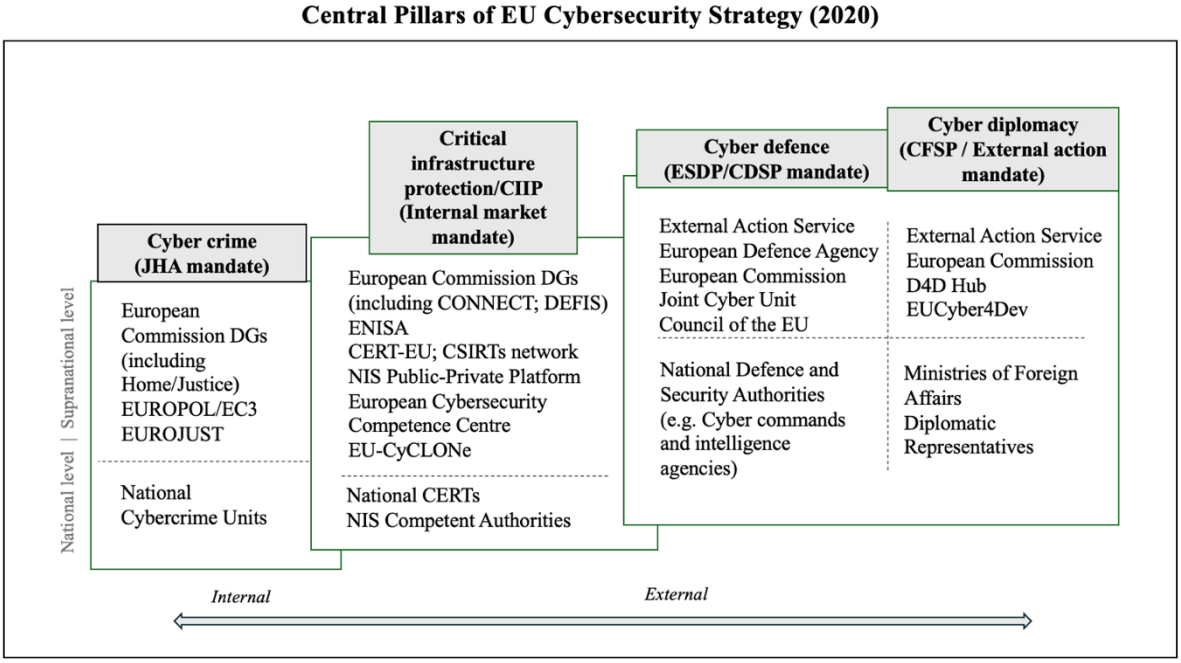


Figure 3.6. Central pillars of the EU's 2020 cybersecurity strategy (in force) and relevant institutional actors, compiled on the basis of the author's institutional mapping and updated for 2020 in line with the European Parliamentary (2024) staff document.

Mapping these broad developments in EU cybersecurity policy raises questions about which kinds of capacities are being privileged by foreign policy actors in the area of cybersecurity, which key ideas and institutions have influence, and which goals they serve; ultimately informing the research agenda of this thesis project addressed in Chapters 4-6.

Particularly relevant to this project is the rise of the EU's behaviour as a geostrategic actor, whereby claims to 'European digital sovereignty' have been popularized under the 2019 von der Leyen Commission (Haroche, 2023; Carrapico & Farrand, 2024). Below, I provide descriptive statistics which demonstrate a key development of interest to this thesis: the convergence of EU sovereigntist discourse and its relationship to EU cybersecurity policy developments from 2009-2024.

The rise of cybersecurity and sovereigntist logics in EU policy documents

The below descriptive analysis provides further insights about the wider discursive environment in which 'European digital sovereignty discourse' has emerged in the context of EU cyber policies over time. This data offers a broad illustration of how EU cybersecurity issues have become increasingly prevalent in a variety of EU documents, including those relevant to international affairs and documents which include references to 'digital sovereignty' and 'technological sovereignty' (further discussion in Appendix A.2).

Prior to examining this development, it is worth noting that 'cybersecurity' policies and issues have risen on the EU's overall policy agenda over the last two decades, particularly since 2016. Textual data collected from the EURLEX database, a repository of all EU public and legal documents,[50] reveals a rising number of EU policy documents containing the keywords 'cybersecurity' and 'cyber security' since 2009 (see Figure 3.7). This demonstrates the rising significance of cybersecurity issues across various EU policy areas over the last two decades. Further, as Figure 3.8 visualizes below, this trend is evident for both document types: those in the preparatory process of EU legislation (e.g. Commission proposals, JOIN documents, Council common positions, European Parliament resolutions) *and* EU legal acts (i.e. EU regulations, decisions, directives, recommendations and opinions). Therefore, over time, the salience of cybersecurity issues has risen across a variety of EU institutions with different policymaking responsibilities. Overall, it shows how cybersecurity has become 'one of the most influential policies across the EU policy spectrum,' (Carrapico & Farrand, 2024, p. 147).

[50] The EURLEX database is a digital repository of all EU law documents and public (policy) documents. This includes treaties, directives, regulations, decisions, preparatory acts, and *The Official Journal of the European Union.* For further details, see: https://eur-lex.europa.eu/content/welcome/about.html#:~:text=What%20is%20EUR%2DLex%3F,languages%20and%20is%20updated%20daily.

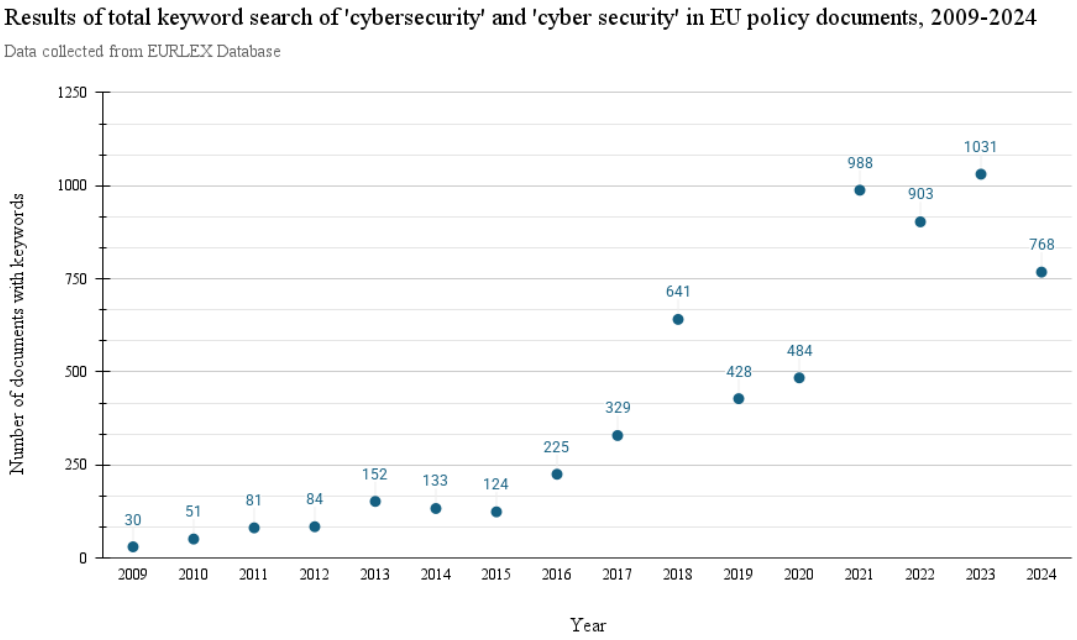


Figure 3.7. Results of keyword search of 'cybersecurity' and 'cyber security' in all EU policy documents over 2009-2024, collected from EURLEX database. Database last accessed February 2025.

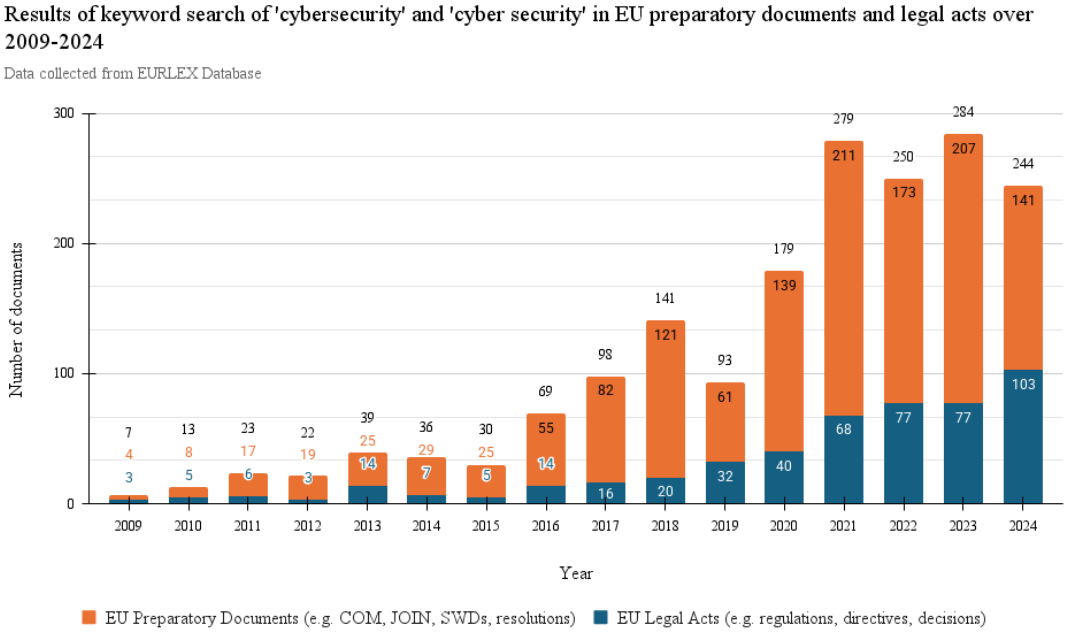


Figure 3.8. Results of keyword search of 'cybersecurity' and 'cyber security' in EU preparatory documents and EU legal acts over 2009-2024, collected from EURLEX database. Database last accessed February 2025.

Focusing more closely on external action and/or international issues, cybersecurity keywords have more frequently appeared in EU documents discussing ‘international relations’ themes over time.[51] This is demonstrated in Figure 3.9 below.

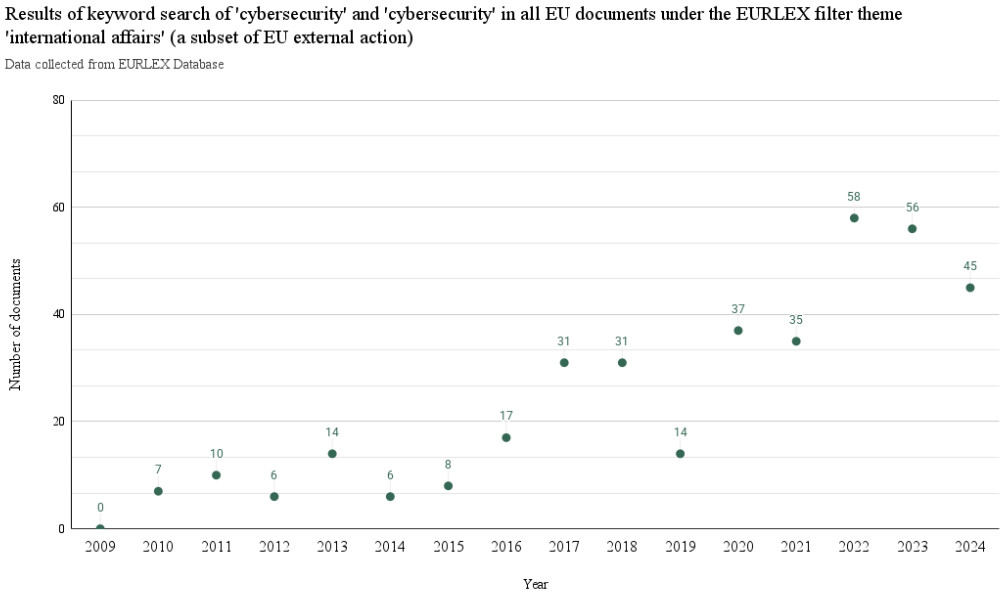


Figure 3.9. Results of keyword search of 'cybersecurity' and 'cyber security' in all documents under the EURLEX filter theme ‘international relations’ with keywords, 2009-2024. Database last accessed February 2025.

Most relevant to the EU’s expression of digital sovereignty discourse in the area of cyber-external action, the data reveals a relative increase in EU documents containing both EU cybersecurity keywords and European digital sovereigntist discourse. This is shown in Figure 3.10, which illustrates that the total number of EU documents containing both the ‘cybersecurity’ and ‘digital sovereignty’ or ‘technological sovereignty’ keywords has increased over time, particularly since 2020.

[51] EU documents were coded ‘Internal relations’ by EURLEX filters, not my own coding; see Appendix A for further information about EuroVoc and the filters used.

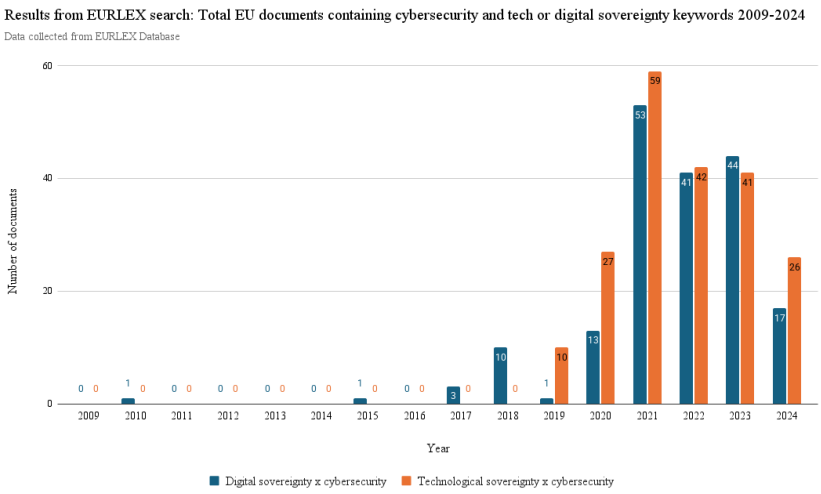


Figure 3.10. Total EU documents including both cybersecurity and tech or digital sovereignty keywords, 2009-2024- last accessed February 2025. The two categories are not mutually exclusive.

Significantly, this association is reflected in both EU legal documents and legislation, as evidenced below, in Figures 3.11 and 3.12. This suggests that, at a very broad level, a variety of different EU supranational institutions (e.g. the European Commission and the European Parliament) and intergovernmental bodies (i.e. the Council of the EU) have engaged with sovereigntist discourses in the context of EU cybersecurity policy.

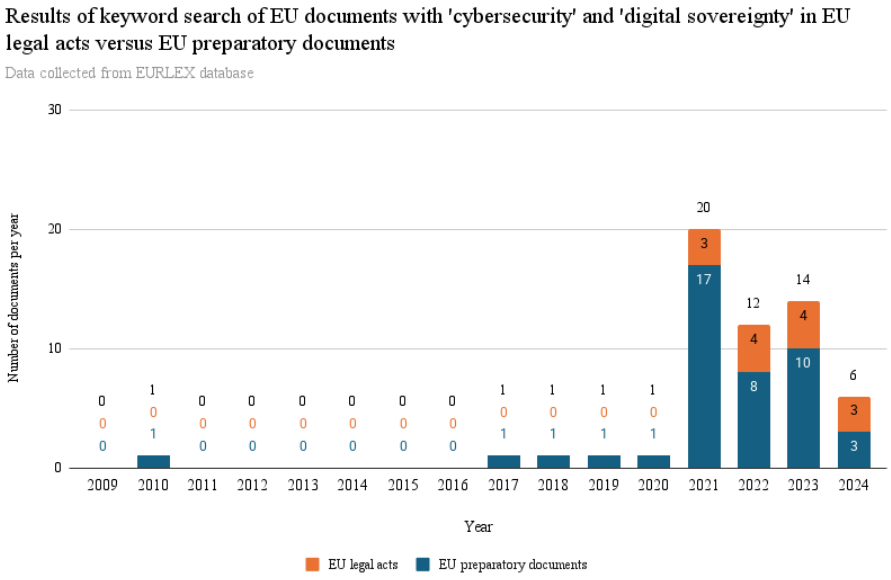


Figure 3.11. Number of EU legal acts and preparatory documents with both cybersecurity and digital sovereignty keywords, 2009-2024 (a subset of data corpus from Figure 3.10). Database last accessed February 2025.

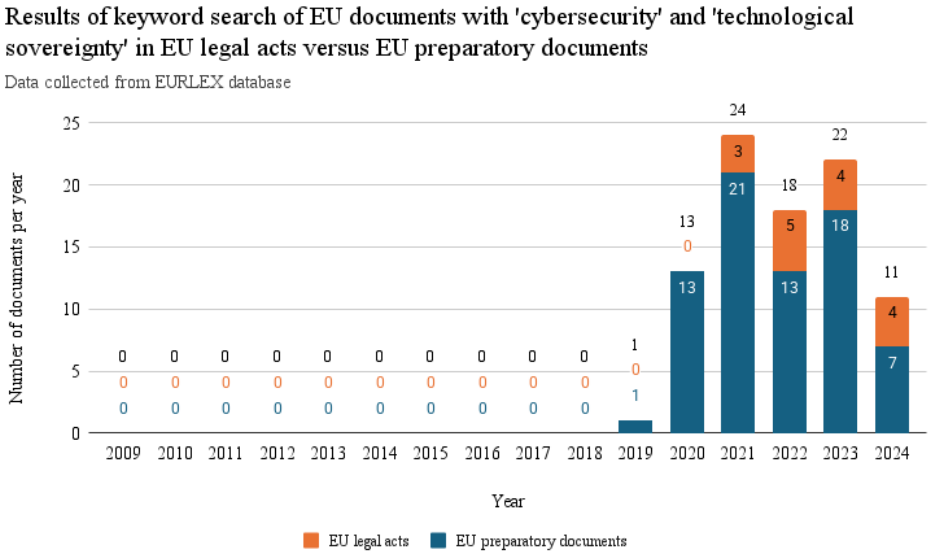


Figure 3.12. Number of EU legal acts and preparatory documents with both cybersecurity and technological sovereignty keywords, 2009-2024 (a subset of data corpus from Figure 3.10). Database last accessed February 2025.

Overall, these data trends illustrate that 1) EU cybersecurity issues have become more salient over time, and 2) sovereigntist logics (i.e. the terms 'digital sovereignty' and 'technological sovereignty') have become more prevalent in EU documents which also reference cybersecurity issues. At least on paper, this exercise notionally supports the argument that the EU's geostrategic agenda, including digital sovereignty discourse, can be understood as 'the new paradigm of EU cybersecurity policy' (Carrapico & Farrand, 2024, p. 148). However, this descriptive analysis offers a very preliminary indication that EU cybersecurity issues have become more prominent in EU external action policy, and that the EU's engagement with geostrategic concepts—namely sovereigntist discourse--has increased over time in this context, across a range of EU document types.

As I detail below, this thesis moves beyond the broader discursive environment to qualitatively examine the meaning of and application of these terms in specific institutional and policy contexts. In the remaining part of this chapter, I lay out the empirical scope and the epistemological, analytical, and methodological 'toolkit' leveraged by the dissertation's research articles.

Empirical coverage and scope of articles

Chapter 1 introduced the central research question guiding this project: *What explains and characterizes geostrategic behaviour in and through cyberspace, and what are the implications of these dynamics for the nature of sovereignty and geopolitics in the digital age?* This thesis addresses this overarching research question in the form of three standalone yet substantially related articles. Valuably, an articles-based approach enables me to address this agenda along the lines of the three related gaps in the literature identified in Chapter 2 (see Table 3.4 below).

Table 3.4. Summary of research lacunae addressed by the thesis and their empirical scope

Gaps	Chapter	Empirical context
The potential relationship between 'capacity' and geostrategic behaviour in and through cyberspace; the meaning of 'capacity' in policy practice(s)	Chapter 4	Capacity building instruments for digital development donated by the EU, US, and China to African states, 2017-2024
The relationship between sovereigntist discourse and policies towards (geospatial) control, especially in the case of the EU	Chapter 5	The relationship between European digital sovereignty discourse and cyber-relevant policy developments in EU external action, 2017-2022
The ontological security dimension to geostrategic decision-making in and through cyberspace	Chapter 6	Emergence of the EU's geostrategic behaviour in EU's cybersecurity policy, as developments in EU external action over 2009-2024
Explaining the EU's emergence and characteristics as a geostrategic actor in and through cyberspace, within the wider context of global competition	Chapters 4-6	Various policy areas in EU external action, different EU actors (including Member States and supranational institutions) and the EU's relations with the US and China

Briefly, by exploring these gaps, my articles unveil the key ideas, events, and forces which have shaped the relationship between transformations to cyberspace and national and supranational practices of geostrategic competition. Specifically, Chapter 4 explores tripartite geopolitical competition between the EU, US, and China at the macro level. Departing from Chapter 4's discussion about institutional and ideational factors which shape

networked geopolitical competition, Chapter 5 zooms in on the EU external action policymaking context to interrogate the meso-level dimension to drivers of cyber capacity building policy and two other policy areas. In so doing, this article explores how institutional competences and ideational factors shape policy changes penned by the 'geopolitical Commission' from 2017-2022. This sheds further light into how cybersecurity policymaking is embedded within the broader politics of geostrategic competition, particularly debates about European digital sovereignty and the EU's role as a global actor in the digital domain. Finally, Chapter 6 examines the ontological security underpinnings of the EU's discursive turn towards geopolitics and European sovereignty over the 2009-2024 period, organized around successive updates to the Union's cybersecurity strategies and external action / strategic doctrines.

Accordingly, Chapters 4-6 of this dissertation examine three (out of four) EU cybersecurity pillars in particular: *cyber defence* and its overlap with *network and information security*, and *diplomacy,* although the fourth pillar, *cybercrime,* is mentioned indirectly in the context of cyber capacity building programmes (see Figure 3.6 above). Given that Sino-American competition is widely acknowledged to have a bearing upon the EU's geopolitical positioning, the research articles also touch upon specific areas of American and Chinese foreign policy when relevant and appropriate to the article's research objectives. Specifically, Chapter 4 examines all three actors as competing digital development donors towards Africa, whereas Chapters 5 and 6 focus more specifically on aspects of the EU's embrace of its distinctive geopolitical, sovereigntist approach to cyberspace. The reasons for the selection of these areas are further elaborated in Chapters 4-6 in the context of their research designs.[52]

[52] Broadly speaking, however, 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, these three pillars comprised the areas in which the EU's adoption of geopolitical discourse and

Altogether, this empirical approach remains alive to the reality that the EU's external relations approach has been shaped by a number of internal and external developments over the 2009-2024 period, including the behaviour of the Union's longtime allies, partners, and competitors. These aspects will be addressed in greater detail in the coming chapters, but it is worth briefly mentioning that the EU has had a longstanding partnership with the United States on governance issues related to cybersecurity, digital technologies, and transnational data flows (see for example Shahin, 2024; Fahey, 2024). Additionally, the EU's external action approach to cyberspace has been shaped by relations with China (see for example Bersick et al., 2016), including in the context of Chinese-provided ICT infrastructure across the bloc, and by external threat perceptions about Russian cyber operations (Christou, 2016).

Overview of analytical approaches and methods for data generation

As I outlined in the preceding chapter, a key point of departure of the thesis was to explore the field's conception of the 'capable actor' in cyberspace in theory and practice through a critical ontological approach. Through this lens, I argued that dominant approaches have produced limited understandings about recent developments in cyberspace assumed to be explained by the exercise (or not) of particular cyber capabilities, particularly the EU's development as a geopolitical actor. Moreover, the field's reliance upon assumptions about power and capabilities in cyberspace come into tension with commonly understood characteristics of the cyber environment, changing geopolitical dynamics, and the EU's development as a geopolitical cyber actor. This broad approach and the emergent research

---

sovereignty claims are concentrated. 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, cyber diplomacy, and network and information security—the inclusion of the all three pillars are warranted.

imperatives and gaps laid out in Chapter 2 comprise the analytical backdrop to the dissertation's three research articles.

As prefaced in Table 3.4, the dissertation's research articles are distinct in terms of their specific research questions, approach to causality, and empirical coverage, drawing upon a range of relevant theoretical tools to pursue their research questions.[53] Broadly speaking, Chapters 4 and 5 develop qualitative, analytical frameworks which aim to empirically investigate causal relations relevant to the EU's geostrategic approach in and through cyberspace, in line with their research questions. As context-specific, theory building exercises, the articles do not advance monocausal or universal explanations, and they highlight the relationship between ideas and the institutional and/or structural context. By contrast, Chapter 6 develops a constitutive, qualitative-interpretive approach towards examining the relationship between the EU's ontological security drives and its spatial bordering practices in and through cyberspace, drawing upon sociopsychological theories in international relations.

In brief, Chapter 4 develops a theoretical framework about the strategic import of capacity building assistance, drawing upon network theory (e.g. Hafner-Burton, et al., 2009) and critical approaches to digital geopolitics (e.g. Pohle & Voelsen, 2022). This chapter engages in a plausibility probe of American, Chinese, and EU-funded capacity building assistance for African states' digital development to explore how several supply-side factors (perceived incentives for competition, donors' normative approaches to development, and their relationship to intermediaries) appeared to mediate donors' approaches to assistance. Next, Chapter 5 engages an 'explaining-outcome' process tracing approach (Beach & Pederson, 2019; see also Haroche, 2022), which seeks to examine whether European digital sovereignty discourse drove three positive cases of policy change in EU cyber-external

[53] Refer to Chapters 4-6 for specific details.

action. Given that this approach does not seek 'to demonstrate the general validity of one causal mechanism but rather to identify the main drivers behind a single phenomenon, this research strategy typically combines multiple theoretical approaches,' (Beach and Pedersen, 2019, p. 282, in Haroche, 2022). As I discuss in this Chapter, this abductive approach enabled me to consider, albeit to a limited extent, whether the paper's empirical findings about the relationship between discourse and policy change are illustrative of several different potential theorized causal pathways (dynamics 1, 2, 3, or 4) and in terms of broader scholarship on EU foreign policymaking.[54]

Departing from Chapter 5's short discussion about the potentially significant performative nature of digital sovereignty discourse, the final article of this dissertation (Chapter 6) examines how ontological security drives may have shaped the EU's geostrategic turn towards cyberspace. This article advances a qualitative-interpretive research approach which draws upon critical geopolitics and EU Studies scholarship (e.g. Lambach, 2020; Klose, 2018; 2022). An interpretive approach emphasizes the constitutive nature of language as 'ontologically significant' for an actor's identity and sense of the world (Hansen, 2006, p. 16), and the crucial role of subjectivity, situated-ness, and contingency for knowledge formation (Schwartz-Shea & Yanow, 2012).[55] In particular, this article develops

[54] As I note in Chapter 5, rather than exploring four hypotheses evenly, the paper is anchored around exploring the evolution of discourse and its temporal sequencing vis-à-vis the outcome (Beach & Pedersen, 2019, p. 286). By exploring whether European digital sovereignty discourse was necessary for driving each of the three cases, the paper further considers, albeit to a limited extent, also other potential variables (such as geopolitical perceptions, transformative crises, and institutional characteristics) and explore how they might have contributed to the outcome. These factors are explored in its analyses of policy changes and in the paper's discussion section. In this section, it also allowed me to briefly consider how, and why, discourses about digital sovereignty may serve both internal and external purposes depending upon the institutional context: for example, the discourse may internally serve as an 'autobiography' or 'solution' for a policy problem, and/or as externally expressing a preferred narrative or vision for an actor's role and perception of world affairs.

[55] Throughout my analytical process, I adhered to five widely recognized evaluative standards for interpretivist research: 1) exposure, 2) trustworthiness, 3) systematicity, 4) transparency, 5) reflexivity and engagement with positionality (Schwartz-Shea & Yanow, 2012). To achieve exposure, I examined different institutional contexts and policy areas appropriate to the research problem (broadly reviewed above), identifying relevant sites for analysis through a temporalized mapping technique, which traces and situates the ideational positions of actors located in different policy settings (Clarke et al., 2015). Together with the interview data (described above), this chronological mapping process facilitated further exposure to the perspectives of the multitude of agents involved in shaping and disseminating the relevant foreign policies (Clarke et al., 2015). The mapping

a critical analytical framework which theorizes the constitutive relationship between the EU's ontological security drives, its collective actorness in and through cyberspace, and its engagement with spatial bordering moves, including digital sovereignty discourse. By drawing upon the concept of actorness, this approach underscored how the EU's geostrategic turn has been shaped by both internal and external social contexts which 'emerges from the interplay of (domestic and external) role expectations, creative action and (social and material) resources' (Klose, 2018, p. 1145). It should be noted, however, that interpretivist approaches do not aim to produce 'universal truths' applicable to the entire 'universe of cases.' Rather, they seek to hone in on a significant tension within a particular context and/or set of contexts (i.e. the EU's puzzling geostrategic turn in cyberspace) which can help build our understanding about important social science phenomena.

Therefore, through distinctive analytical frameworks and epistemologies, Chapters 4-6 explored both discourses and practices relevant to and indicative of the EU's geostrategic behaviour in and through cyberspace. Through different angles of inquiry, the discourse-oriented approaches of these articles enabled me to explore how 'capacity', 'cyberspace' and 'the digital domain' have been shaped and constituted by ideational factors across various (evolving) political, institutional, and temporal contexts. As a point of departure for their discourse analyses, the articles engaged with Bacchi and Goodwin's (2016) 'WPR' Analysis tool to identify the key ideas, institutions, and concepts pertinent to the relevant policy issues for the analysis. WPR, or 'What is the Problem Represented to Be?', is a critical exercise which elicits a sequence of questions for 'opening up policies' for discourse analysis (see Figure 3.13 below*).* WPR approaches policies as discursive problematizations of issues which produce "problems" as particular *types* of problems, to therefore uncover the

process also enabled me to establish appropriate analytical parameters for my interpretive analysis of the broad policy field of 'cybersecurity' and its co-evolution with geopolitical behaviour, which has expanded over time in most foreign policy contexts, including the EU.

underlying assumptions which construct such "problems" as intelligible (Bacchi & Goodwin, 2016).

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?

Figure 3.13. Excerpt from Bacchi and Goodwin's (2016) volume, reproduced by the author.

For Chapter 4, in line with its two-step analytical framework, discourse analysis served as a preliminary step for elucidating American, Chinese, and European perceptions and framings about the strategic importance of cyber and digital capacity building assistance and their relationship to wider dynamics of networked competition. Similarly, analysing the EU's evolving discursive approach towards cyberspace was a crucial first step for the research objectives of Chapter 5, which developed an abductive analytical framework to assess whether and how digital sovereignty discourse drove three significant cybersecurity policy changes in the EU's cyber-external action domain. This framework draws from discursive-institutionalist approaches which emphasize the importance of (subjective) ideas and the significance of the institutional context in which these ideas are expressed (Schmidt, 2008, p. 305).[56] Furthermore, in Chapter 6, discourse analysis was central to the article's

[56] As reviewed in this chapter, the institutional context of EU policymaking varies significantly across different policy areas (e.g. between the CFSP vs. trade policy). Emphasizing the interactive relationship between structure and agency, Chapter 5's approach explores how policy discourses, for example about sovereignty and geopolitics, can have varying effects and relationships to an actor's concrete policy actions (see also Hall, 1993). This facilitates scrutiny of the interaction between ideational and structural factors, 'with institutions and culture framing the discourse, defining the repertoire of acceptable (and expectable) actions,' (Schmidt & Radaelli, 2004, p. 193). Given that discourse constitutes a web of 'policy ideas and values' negotiated and contested by policy actors (Schmidt & Radaelli, 2004, p. 184), policymakers might deem some discursive

qualitative-interpretive approach, which underscored the constitutive relationship between the EU's self-narratives (a form of discourse) and its ontological security drives in the Union's external action approach towards cyberspace. Here, discourse analysis was critical for interrogating the ideas and actors constituting the EU's evolving self-narrative(s) about its role(s) as a cybersecurity actor, for example by identifying discursive struggles between different policy communities, such as between EU Member States and across EU institutions (Schmidt, 2011; Hansen, 2006).

Data corpus

Collectively, the thesis articles draw upon a wealth of qualitative primary and secondary sources, from policy documents, to meeting minutes, to elite interviews. Primary source documents leveraged by this dissertation 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), among others. Documents were extracted from digitized archives, most frequently the EURLEX database, EU and Member State websites, and from relevant think tank and policy organizations. This dissertation also leveraged extant freedom of information requests related to EU external action, including internal EU reports related to the EU Cyber Defence Policy Framework, retrieved from the AskEU organizational database. 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 exposed further tensions and questions which directed further research.

---

concepts more significant than others for a given policy issue, contest the meaning of competing concepts within a discourse, or conflate the meaning of several similar concepts.

As part of my data generation, I conducted twenty-five formal, semi-structured elite interviews in 2021-2022, and five informal interviews in 2023 and 2024, which yielded approximately 30 hours of qualitative data for analysis. The majority of formal interviewees (20) were drawn from European governmental institutions (at the national and supranational levels), and these data were supplemented by formal interviews with five policy experts. The below figure (Figure 3.14) visualizes the positionalities of the twenty-five *formal* interviews with European policy elites (20) and policy experts (5) relevant to the EU policy community.

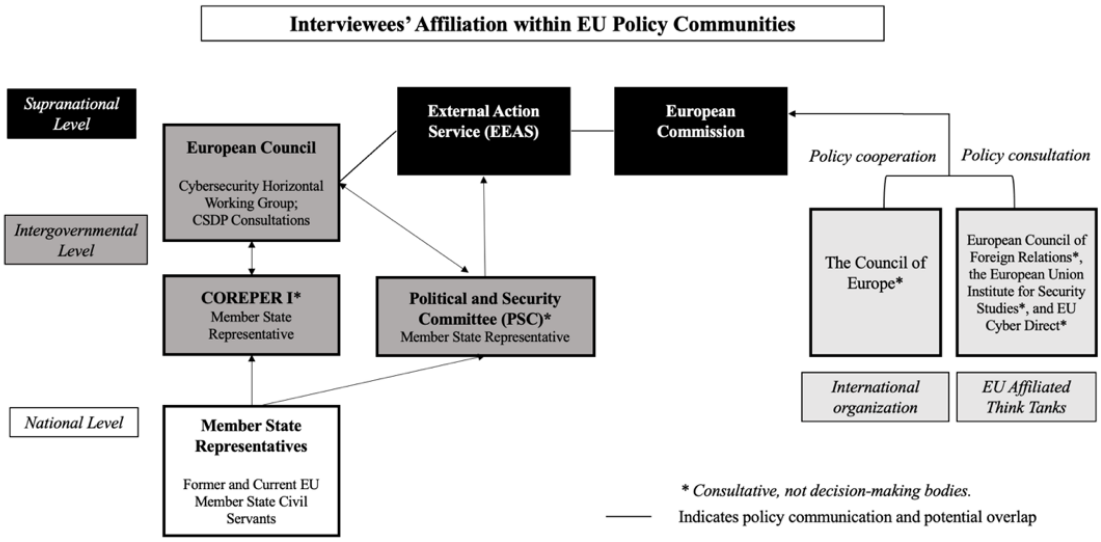


Figure 3.14. Schematic of formal European interviewees' positionalities. Figure excludes informal interviewees and American and British participants.

Interviewees held a variety of different levels of seniority and professional expertise, with several serving as the primary authors of important strategic documents for EU cyber external action policy. Additionally, as the project further developed (and cyber policy developments progressed) over time, I conducted five additional background interviews to inform my documentary analysis, which were carried out 'off the record.' I carried out two informal interviews in 2023 with European policy experts, and three informal interviews with US and UK-based practitioners and policy experts in 2024.

Interviews were particularly valuable for exposing contestation, internal views on policy issues, and explaining rapid policy developments pertinent to Chapters 5 and 6. For example, in the case of Chapter 5, interviews enabled me to further explore the possibility of 'invisible' ideational contestation and overlap and elucidate how European digital sovereignty discourse shaped and was shaped by policymakers' worldviews. The formal interviews of EU policymakers enabled me to uncover internal institutional dynamics relevant to the policy change process and for identifying areas of discursive struggle within or across policy settings not visible in official EU policy or strategy documents. This data, in turn, was important for probing the relationship between European digital sovereignty discourse and other causally relevant factors which appeared to bear upon the process of policy change. In Chapter 6, they were valuable for identifying how policymakers discursively represented the EU's external action in and through cyberspace, including discursive chains of association[57] linked to the EU's self-representation vis-à-vis 'Others' in the cyber environment.

Notably, the relationship between 'thinking, saying and doing' is often challenging to gauge, as agents may not say or do what they're thinking, and vice versa (Schmidt 2011, p. 115). Yet, as Greenstein and Mosley observe, 'interviews provide rich and oftentimes surprising data that cannot be obtained in any other way, and, when used properly, they can shape and support work that is both rigorous and innovative,' (2020, p. 1167). Here, I employed the technique of intertextuality to corroborate—and compare—information expressed by an agent in a private interview in comparison to the 'official line' (see also Schwartz-Shea & Yanow, 2012). Intertextuality is the process of situating texts within and against other texts to reveal how one particular source (e.g. a strategy document) is embedded within the broader political and social discourse (Hansen, 2006). For example, in

[57] For further details, see Chapter 6.

Chapter 5, intertextuality was adopted to elucidate key constitutive concepts of European digital sovereignty discourse, trace the mainstreaming and updating of particular texts over time (such as updates of the EU's cybersecurity strategy) and identify policy contexts whereby the discourse was officially absent. Data were analysed for how they represented policy issues as particular types of problems (e.g. WPR; Bacchi & Goodwin, 2016) in order to examine the extent to which digital sovereignty discourse was understood to be relevant and/or applicable to a particular policy instrument or issue. Next, clearly and thoroughly documenting my analytical processes, as described here and in the articles, facilitates *systematicity* and *transparency*. Finally, coherent with my reflexive, ontological approach, and my interpretive framework for Chapter 6, I remained alive to my positionality as a female doctoral student at Oxford.[58]

As I discuss in the following chapters, the scope and methodological orientations of the project limit the generalisability of the thesis' empirical findings. Yet, the primary goal of this study is not to develop 'universal truths' about a phenomenon, or the 'facts' about sovereignty or geopolitics at large. Nor do I assume that EU policymakers (for example) understand geopolitics in the same way as national policymakers, or indeed scholars operating within particular theoretical frameworks. Beyond this study, developing

[58] In 2021, I founded a cyber strategy working group based at Nuffield College which invited both practitioners and academics to discuss policy-relevant challenges pertinent to cyber strategy, including geopolitics, escalation, and concepts of 'responsibility.' This group, which was affiliated with the Oxford Changing Character of War Centre, met regularly (biweekly) for two years and acted as a focus group for a variety of challenged 'cyber' questions for foreign policy, security, and strategy. By leading the group and managing the invitation list, I was exposed to a variety of perspectives from practitioners and policy experts on issues relevant to my own research, including views from the UK's GCHQ, DSIT, and Ministry of Defence, as well as British and American military officers. More recently, in 2024, I have been working as a Research Associate for the Global Cyber Security Capacity Centre (GCSCC) based at Oxford's Department of Computer Science and the Oxford Martin School. In my role as a GCSCC researcher, I engage directly with foreign governments and representatives from the UK's FCDO to identify cybersecurity challenges and evaluate the country's cybersecurity maturity on the basis of a globally recognized model for evaluation. These experiences have provided me with invaluable exposure to the European, Latin American, and American 'cybersecurity communities of practice', in a variety of different institutional and socio-political contexts, for the past three years. As a result, I have been privileged to have intimate access to conversations, ideas, and issues relevant to the thesis which would not have been possible at my desk alone. These experiences have provided me with valuable situational context to inform my data generation and theory building.

‘complete’ or ‘conclusive’ depictions of the rapidly proliferating, ambiguous, and complex institutional scale of ‘cyber-IR’ is one of the central and enduring challenges of the discipline (Dunn Cavelty & Wenger, 2019).

Nonetheless, this study seeks to contribute to our understanding of the bigger picture through an in-depth exploration of three key gaps in the study of cyber-geopolitics. In so doing, it foregrounds several largely overlooked yet significant empirical contexts, policy changes, and events pertinent to the EU’s development as a geopolitical actor in cyberspace. The articles, furthermore, develop novel theoretical and analytical tools for approaching geostrategic behaviour—some of which have arguably wider applications beyond the EU (as will be detailed in Chapter 4).

Chapter summary

This chapter provided a broad overview of the EU’s institutional makeup and external action policy priorities, offering further contextual background about the EU as a foreign policy actor. It also highlighted the rising salience of cybersecurity issues in EU policy, and their convergence with the EU’s engagement with sovereigntist discourse in various EU policy documents. Additionally, it laid out the scope of articles, which examine policy developments in the context of EU external action towards cyberspace over the 2009-2024 timeframe through distinct qualitative, analytical approaches. In turn, I elaborated the methodological orientation of the integrated thesis in very general terms. The next three chapters comprise the substantive research articles of the thesis.

Chapter 3 References

Balfour, R., C. Carta, & K. Raik (Eds). (2015). *The European External Action Service and Foreign National Ministries. Convergence or Divergence*? Surrey: Ashgate.

Bartolini, S. (2006*). Restructuring Europe: Centre formation, system building, and political structuring between the nation state and the European Union*. Oxford University Press.

Bauerle Danzman, S., & Meunier, S. (2024). The EU's geoeconomic turn: From policy laggard to institutional innovator. *JCMS: Journal of Common Market Studies, 62*(5), 1097–1115. https://doi.org/10.1111/jcms.13599

Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines.* University of Michigan Press.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security, 31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Berenskoetter, F. (2017). Approaches to Concept Analysis. *Millennium: Journal of International Studies, 45*(2), 151-173. https://doi.org/10.1177/0305829816651934.

Bersick, S., Christou, G., & Yi, S. (2016). Cybersecurity and EU–China Relations. In E. J. Kirchner, T. Christiansen, & H. Dorussen (Eds.), *Security Relations between China and the European Union: From Convergence to Cooperation?* (pp. 167–186). chapter, Cambridge: Cambridge University Press.

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue, 44*(2), 147–164. http://www.jstor.org/stable/26302224.

Bourdieu, P., & Wacquant, L. (1992). *An invitation to reflexive sociology*. Polity Press.

de Búrca, G. (2013). EU external relations: The governance mode of foreign policy. In B. Van Vooren, S. Blockmans, & J. Wouters (Eds.), *The EU's role in global governance: The legal dimension* (Chap. 3). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199659654.003.0004.

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *JCMS: Journal of Common Market Studies, 62*, 147–158. https://doi.org/10.1111/jcms.13654.

Clarke, A. E., Friese, C., & Washburn, R. (2015). *Situational analysis in practice: Mapping research with grounded theory*. Routledge, Taylor and Francis.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy.* Palgrave Macmillan.

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the

making: the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy,* 30(7), 1330–1352. https://doi.org/10.1080/13501763.2023.2173274.

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41(*1), 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Dunn Cavelty, M., & Wenger, A. (Eds.). (2022). *Cyber security politics: Socio-technological transformations and political fragmentation.* Routledge.

European Parliament. (n.d.). The EU's external relations. Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/chapter/213/the-eu-s-external-relations.

Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: on drivers of convergence. *Journal of European Integration, 46*(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240.

Fawcett, L. (2015). *Drivers of regional integration: Historical and comparative perspectives*. Routledge.

Fossum, J. E. (2006). Conceptualizing the European Union through four strategies of comparison. *Comparative European Politics, 4*(1), 94–123. https://doi.org/10.1057/palgrave.cep.6110077.

Furness, M. 2013. "Who Controls the European External Action Service? Agent Autonomy in EU External Policy." European Foreign Affairs Review 18 (1): 103–125. https://doi.org/10.54648/eerr2013006.

González-Ocantos, E. (2020). Designing qualitative research projects: Notes on theory building, case selection and field research. In L. Curini & R. Franzese (Eds.), *The SAGE Handbook of Research Methods in Political Science and International Relations* (Vol. 2, pp. 104–120). SAGE Publications Ltd. https://doi.org/10.4135/9781526486387.n9.

Greenstein, C., & Mosley, L. (2020). When talk isn't cheap: opportunities and challenges in interview research. In L. Curini, R. Franzese (Eds.) *When talk isn't cheap: opportunities and challenges in interview research* (Vol. 2, pp. 1167-1189). SAGE Publications Ltd, https://doi.org/10.4135/9781526486387.n64.

Guzzini, S. (2013). The ends of International Relations theory: Stages of reflexivity and modes of theorizing. *European Journal of International Relations, 19*(3), 521-541. https://doi.org/10.1177/1354066113494327.

Hafner-Burton, E. M., Kahler, M., & Montgomery, A. H. (2009). Network analysis for international relations. *International Organization, 63*(3), 559–592. https://doi.org/10.1017/S0020818309090195

Hall, P. A. (1993). Policy paradigms, social learning, and the state: The case of economic

policymaking in Britain. *Comparative Politics, 25*(3), 275–296. http://www.jstor.org/stable/422246.

Hansen, L. (2006). *Security as practice: Discourse analysis and the Bosnian war* (1st ed.). Routledge.

Haroche, P. (2022). A 'geopolitical commission': Supranationalism meets global power competition. *JCMS: Journal of Common Market Studies, 61*(4), 970–987. https://doi.org/10.1111/jcms.13440.

Heidebrecht, S. (2024) From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance. *JCMS: Journal of Common Market Studies, 62:* 205–223. https://doi.org/10.1111/jcms.13488.

Hill, C. (1993). The Capability-Expectations Gap, or Conceptualizing Europe's International Role. *Journal of Common Market Studies, 31*(3), 305–328. https://doi.org/10.1111/j.1468-5965.1993.tb00466.x.

Jessop, B. (1999). The strategic selectivity of the state: Reflections on a theme of Poulantzas. *Journal of the Hellenic Diaspora, 25(*1–2), 1–37.

Keukeleire, S., & Delreux, T. (2022). *The Foreign Policy of the European Union* (Third edition.). Bloomsbury Academic.

Keukeleire, S., & Delreux, T. (2014). *The Foreign Policy of the European Union* (2nd ed.) Basingstoke: Palgrave Macmillan.

Klose, S. (2018) Theorizing the EU's Actorness: Towards an Interactionist Role Theory Framework. JCMS: *Journal of Common Market Studies, 56*, 1144–1160. https://doi.org/10.1111/jcms.12725.

Kurowska, X., & de Guevara, B. (2020). Interpretive approaches in political science and international relations. In L. Curini & R. Franzese (Eds.), *The SAGE handbook of research methods in political science and international relations* (Vol. 2, pp. 1211–1230). SAGE Publications Ltd. https://doi.org/10.4135/9781526486387.n66.

Kuus, M. (2009). Political geography and geopolitics. *The Canadian Geographer / Le Géographe Canadien, 53*(1), 86–90. https://doi.org/10.111.org/j.1541-0064.2009.00238.x.

Laurer, M., & Seidl, T. (2021). Regulating the European data-driven economy: A case study on the general data protection regulation. *Policy & Internet, 13(*2), 257–277. https://doi.org/10.1002/poi3.246.

Morillas, P. (2020). Autonomy in intergovernmentalism: The role of de novo bodies in external action during the making of the EU Global Strategy. *Journal of European Integration, 42*(2), 231–246. https://doi.org/10.1080/07036337.2019.1666116.

Moisio, S., & Paasi, A. (2013). From Geopolitical to Geoeconomic? The Changing Political Rationalities of State Space. *Geopolitics, 18*(2), 267–283. https://doi.org/10.1080/14650045.2012.723287

Moravcsik, A. (1998). *The choice for Europe. Social purpose and state power from Messina to Maastricht.* Routledge.

Pawlak, P. (2018). Operational Guidance for the EU's International Cooperation on Cyber Capacity Building (Report: ISBN 978-92-9198-756-6). *EUISS Task Force for Cyber Capacity Building, European Commission.* https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf).

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the internet and the global digital order. *Policy & Internet,* 14(1), 13–27. https://doi.org/10.1002/poi3.296.

Rupp, C. (2024, June 27). Navigating the EU cybersecurity policy ecosystem: A comprehensive overview of legislation, policies and actors. Interface. https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem.

Shahin, J. (2024). Dancing to the same tune? EU and US approaches to standards setting in the global digital sector. *Journal of European Integration, 46*(7), 1111–1131. https://doi.org/10.1080/07036337.2024.2398430.

Schmidt, V. (2011). Speaking of change: Why discourse is key to the dynamics of policy transformation. *Critical Policy Studies, 5*(2), 106–126. https://doi.org/10.1080/19460171.2011.576520.

Schmidt, V. (2008). Discursive institutionalism: The explanatory power of ideas and discourse. *Annual Review of Political Science, 11,* 303–326. https://doi.org/10.1146/annurev.polisci.11.060606.135342.

Schmidt, V., & Radaelli, C. M. (2004). Policy change and discourse in Europe: Conceptual and methodological issues. *West European Politics, 27*(2), 183–210. https://doi.org/10.1080/0140238042000214874.

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive design: Concepts and processes.* Routledge, Taylor & Francis

Sjöstedt, G. (1977) *The External Role of the European Community* (Farnborough: Saxon House).

Sjursen, H. (2011). Not so intergovernmental after all? On democracy and integration in European Foreign and Security Policy. *Journal of European Public Policy,* 18(8),1078–1095. https://doi.org/10.1080/13501763.2011.615194.

Smith, M. (2012). Still Rooted in Maastricht: EU External Relations as a 'Third-

generation Hybrid', *Journal of European Integration 34*(7); 699-715. https://doi.org/10.1080/07036337.2012.726010.

Timmers, P. (2018). The European Union's Cybersecurity Industrial Policy. *Journal of Cyber Policy, 3*(3), 363–384. https://doi.org/10.1080/23738871.2018.1562560.

Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). Cybersecurity in the EU common security and defence policy (CSDP): Challenges and risks for the EU (Report no. PE 603.175). European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2017)603175.

Vollaard, H. (2018). *European disintegration: A search for explanations.* Palgrave Macmillan.

Zielonka, J. (2011). The EU as an international actor: Unique or ordinary? *European Foreign Affairs Review, 16*(3), 281–301.

Appendix A - Coding information for EURLEX descriptive statistics

Appendix A.1 – Descriptive statistics method

To collect the data for my quantitative analysis, I used the EURLEX 'Advanced Search' function, which enables the researcher to select for documents within a given date range (here: 01/01/2009-31/12/2024) and for particular keywords within the title and main text of EURLEX documents (e.g. 'cybersecurity', 'cyber security', 'digital sovereignty', etc). I provide further information about the database and filters below, which were last accessed in February 2025. Please note that EURLEX's 'Advanced search' functionality may change over time, including in terms of document categorization or filtering.

Filtering to create data subsets

1. **EU document types (e.g. Figure 3.11)**

By leveraging Advanced Search, I filtered the database for particular document types, including preparatory documents and EU legal acts (see table below), as well as particular themes, in line with the Publication Office's thesaurus system, 'EuroVoc' (more details in next section).

Main document types		
'Preparatory documents'	**'EU legal acts'**	**Other selections**
1. Commission legislative proposals 2. Council common positions 3. European Parliament legislative and budgetary resolutions and initiatives 4. European Economic and Social Committee opinions 5. Committee of the Regions opinions** 6. SEC/SWD (Staff working documents)	1. Regulations 2. Directives 3. Decisions 4. Guideline 5. Recommendations* 6. Opinions**	1. EU court cases 2. 'Other' category in EURLEX, including proposal for legal acts, reports, webpages, working documents, draft decisions, etc.
*Numbers 5 and 6 under 'EU legal acts' are non-binding. **Opinions released *during* the legislative process are categorized as preparatory documents.		

Source: European Union, n.d. (https://eur-lex.europa.eu/collection/eu-law/pre-acts.html; https://eur-lex.europa.eu/collection/eu-law/legal-acts/recent.html).

2. **Thematic filters using EuroVoc**

The EuroVoc thesaurus is a controlled vocabulary developed by the EU, which is used by EURLEX to label the content of all EU documents in the EURLEX database. The EuroVoc filter can be used as selection criteria for the 'Advanced Search' function, as I have used for Figure 3.9. According to the EU Publications Office, 'EuroVoc is managed by the Publications Office of the European Union, which moved forward to ontology-based thesaurus management and semantic web technologies conformant to W3C recommendations as well as latest trends in thesaurus standards.' (Publications Office of the European Union, n.d.) The database URL can be found here: http://publications.europa.eu/resource/dataset/eurovoc. I have provided the term specifications for the filters used to collect data below.

Keyword search filter details and specifications for Figures 3.7-3.12, for reproducibility. Parameters are those stipulated by the EURLEX database 'Advanced search', last accessed February 2025.

Figure 3.7:

Domain: All, Date: All dates, From: 01/01/2009, To: 31/12/2024, Results containing: "cybersecurity" In title and text, OR: "cyber security" In title and text, Search language: English

Figure 3.8:

1. For EU preparatory documents (subset): Domain: All, Type of act: COM and JOIN documents, SEC or SWD documents, Date: All dates, From: 01/01/2009, To: 31/12/2024, Results containing: "cybersecurity" In title and text, OR: "cyber security" In title and text, Search language: English
2. For EU legal acts (subset): Domain: All, Type of act: Regulation, Directive, Decision, EU court case, From: 01/01/2009, To: 31/12/2024, Results containing: "cybersecurity" In title and text, OR: "cyber security" In title and text, Search language: English

Figure 3.9:

EURLEX Search Filter :Domain: All, Date: All dates, From: 01/01/2009, To: 31/12/2024, Results containing: "cybersecurity" In title and text, OR: "cyber security In title and text, Eurovoc descriptor Tt: international instrument, defence policy, international affairs, international agreement, EUROVOC descriptor: non-state actors, accession to an agreement, multilateral relations, international sanctions, code of conduct, international aid, official visit, deterrent, framework agreement, relations between the two German States, North-South relations, UN Conference, consulate, rearmament, enlargement of an international organisation, financial compensation of an agreement, summit meeting, ratification of an agreement, United Nations Charter, diplomatic immunity, revision of an agreement, embassy, international meeting, rapid reaction force, new economic order, UN resolution, financial protocol, strategic defence, diplomatic relations, UN convention, defence expenditure, association agreement, diplomatic representation, fact-finding mission, ministerial meeting, diplomatic protection, exclusion from an international organisation, military science, strategic autonomy, European charter, international charter, stationing of forces, military secret, military sanctions, multilateral agreement, bilateral agreement, cooperation agreement, economic relations, diplomatic profession, protective clause, permanent representation to the EU, economic coercion, economic agreement, observer, renewal of an agreement, recommendation, military base, diplomatic protocol, defence budget, withdrawal from an agreement, economic sanctions, transatlantic relations, UN international covenant, European convention, defence statistics, bilateral relations, resolution, international relations, international convention, European defence policy, protocol to an agreement, signature of an agreement, East-West relations, international negotiations, parliamentary diplomacy, European conference, European Convention on Human Rights, international conference, Search language: English

Figure 3.10:

Collation of two searches:

1. Domain: All, Date: All dates, From: 01/01/2009, To: 31/12/2024, Results containing: "digital sovereignty" In title and text, Results containing: "cybersecurity" In title and text, Search language: English
2. Domain: All, Date: All dates, From: 01/01/2009, To: 31/12/2024, Results containing: "technological sovereignty" In title and text, Results containing: "cybersecurity" In title and text, Search language: English

Figure 3.12: Used data collected for Figure 3.8.

Appendix A.2: Data normalization and further discussion

The descriptive statistics produced above focus upon the number of keywords in documents per year. Theoretically, it is possible that this trend may be simply due to the

rising number of EU publications per year (and the average frequency of the discourse remains stable), rather than an increase in the usage of the keywords themselves. To test this, as seen in Figure 3.15 below, I normalized the previous analysis conducted in Figure 3.7 by the number of overall documents published each year, such that the data is now shown as a proportion of the total number of documents published annually. Therefore, Figure 3.15 below demonstrates an upward trend of EU publications containing cybersecurity references, even when accounting for the total number of EU documents published per year. This trend has been corroborated elsewhere by recent quantitative reports (Interface, 2024)[59] and scholarship (Farrand et al., 2024).

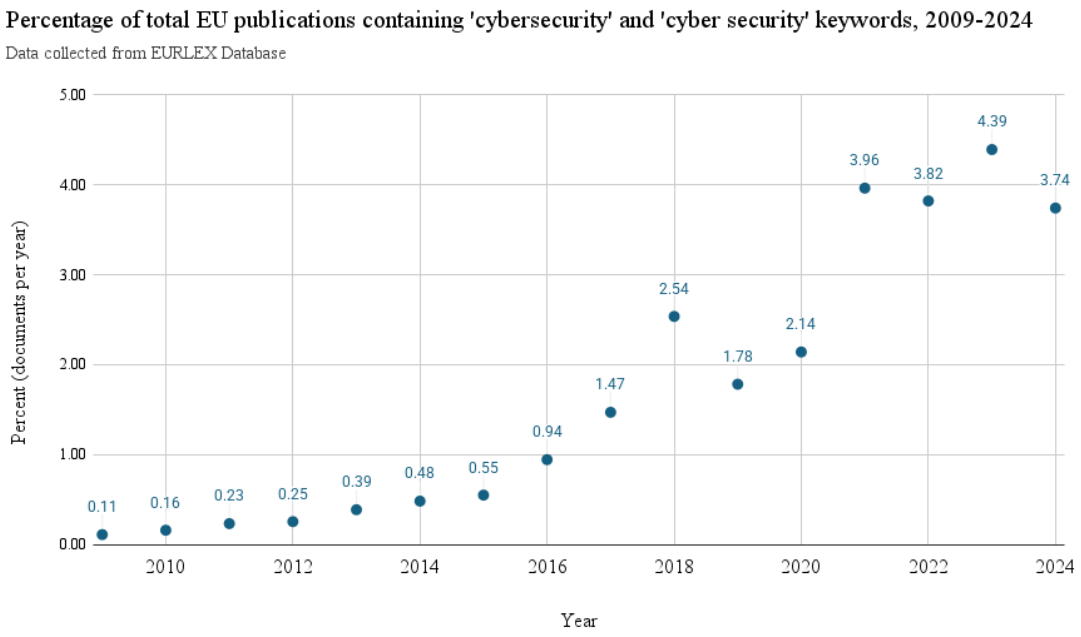


Figure 3.15. Percentage of total EU documents published per year containing 'cybersecurity' or 'cyber security' keywords, 2009-2024.

This is further illustrated by performing the same analysis on a subset of this data: the results of Figure 3.16. The yearly percentage of EU documents containing both

[59] Christina Rupp, Navigating the EU Cybersecurity Policy Ecosystem: A Comprehensive Overview of Legislation, Policies and Actors (Interface, June 27, 2024), https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem.

cybersecurity and tech/digital sovereignty keywords reflects a similar upwards trend: over time, EU documents have increasingly incorporated both cybersecurity and sovereigntist rationales (see Figure 3.16 below). Notably, however, there is one outlier to this trend, in 2010. The 2010 document refers to Member State's digital sovereignty, rather than *European* or collective digital sovereignty, in comparison to the prominence of 'European digital sovereignty' in later periods (e.g. 2019-2024).

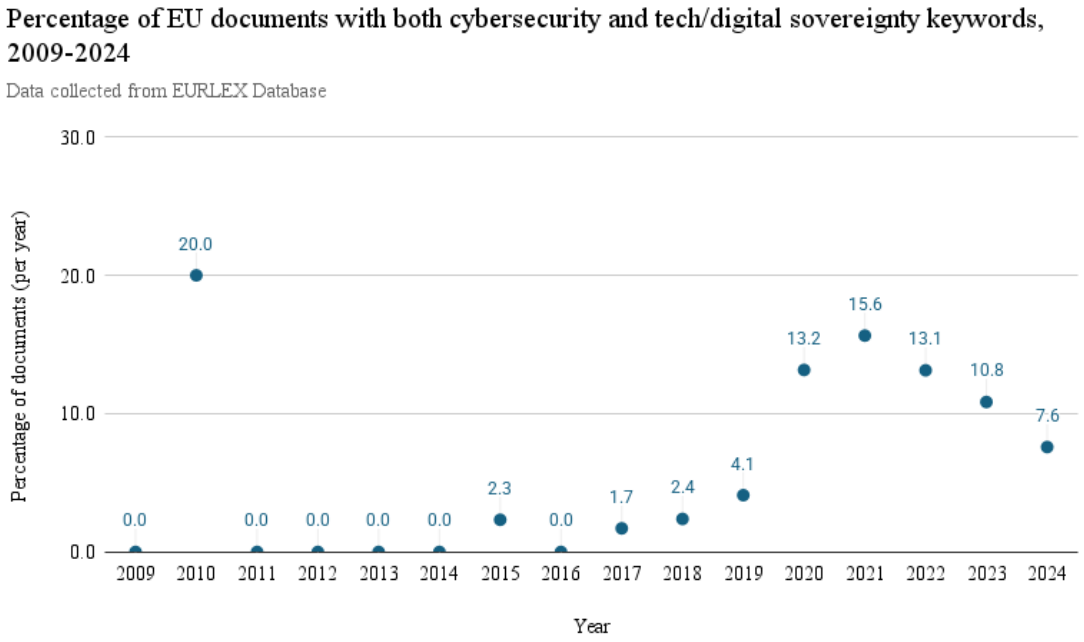


Figure 3.16. Percentage of EU documents with both cybersecurity and tech/digital sovereignty keywords, 2009-2024.

Chapter 4: Developing digital 'peripheries' for strategic advantage: Capacity building assistance and strategic competition in Africa[60]

Abstract

Capacity building (CB) assistance for digital development has climbed the foreign policy agendas of powerful states, yet its strategic significance remains opaque. Particularly, while CB is believed to reduce a recipient's vulnerabilities to weaponized interdependence, three major financiers of such assistance—the United States, China, and the European Union—have all been accused of exploiting global interdependence for strategic gains. How do powerful donors perceive CB assistance provisions as shaping their strategic advantage? Furthermore, which factors have shaped variation in their provision of CB assistance to developing states? This paper argues that donors have perceived CB assistance as a way to outcompete geopolitical rivals and to (re)shape global digital networks through forming strategic alignments. This logic is supported with evidence from American, EU, and Chinese CB for digital development in Africa. By foregrounding CB's strategic dimension, this study contributes to emerging scholarship on (digital) networked, geopolitical competition in the current digital era.

Keywords: strategic competition; digital development; foreign policy; weaponized interdependence; capacity building; cybersecurity

[60] This article has been published. See Carver, J. (2024). Developing digital "peripheries" for strategic advantage: Capacity building assistance and strategic competition in Africa. *Contemporary Security Policy,* 46(3), 455–496. https://doi.org/10.1080/13523260.2024.2430021.

Introduction

Fears about weaponized interdependence and state capacity gaps have come to characterize the contemporary international security environment (Cha, 2023; Collett & Barmpaliou, 2021; Drezner et al., 2021). As governments try to keep pace with global digital transformations, they have allegedly fallen prey to Chinese "debt trap diplomacy" (Pence, 2018), "abusive" American hegemony (Ministry of Foreign Affairs of the People's Republic of China, 2023), and great power "digital neocolonialism" (Gravett, 2022). These worries are particularly acute for African states, which remain plagued by unequal connectivity, lagging cybersecurity governance, and multiple cybersecurity skills gaps (Ramim & Hueca, 2021; Narlikar, 2021). Recently, the African Union declared that building state capacity in cyberspace has become a major "precondition" for the continent's digital transformation, helping "to secure [the continent's] cyberspace" and preserve African states' digital sovereignty (2020, pp. 17, 46). Consequently, African governments have turned to capacity building initiatives provided by foreign donors, which may range from training in cybersecurity skills, sharing best practices for cyber resilience and e-governance, and funding improvements in digital connectivity and critical infrastructure (Hathaway & Spidalieri, 2021).

Prevailing wisdom in the international security literature suggests that—at least from a donor's perspective—such agreements are fraught by a paradox. On the one hand, capacity building assistance is held to be crucial for improving the recipient's adaptability and resilience in the world; to empower communities to prosper in the digital age (Hathaway & Spidalieri, 2021; Pawlak, 2014). On the other hand, powerful actors—often the providers of such assistance—are believed to benefit from the same networked vulnerabilities that these programs aim to redress (Farrell & Newman, 2019). Indeed, three major financiers of digital development assistance—namely, the United States (US), China, and the European Union

(EU)—stand accused of exploiting network asymmetries for their own strategic advantage (Drezner, et al., 2021). As one US State Department official acknowledged, "Capacity-building programming is not always the "sexiest" aspect of international security policy, but it's extremely important—and it is part of how policy translates into real-world outcomes"—such as increasing US "competitiveness against great power challengers" (Ford, 2020).

In this debate, China's Belt and Road Initiative (BRI) has attracted considerable scrutiny (Hall & Krolikowski, 2022). However, it remains unclear how *capacity building assistance* tools within the context of digital development cooperation are perceived by Washington, Brussels, and Beijing as enablers for projecting influence. Given this gap in the literature, this article asks: how do powerful donors perceive the provision of capacity building assistance for digital development as shaping their strategic advantage? Further, which factors have shaped variation in donors' provision of such assistance to developing states?

In this article, I chiefly argue that the provision of capacity building (CB) assistance for digital development has been perceived by donors as creating opportunities to position themselves favorably in the global digital environment and to hedge against geopolitical rivals. Drawing upon IPE, development, and security assistance literatures, I theorize that such assistance can be understood as a form of strategic alignment and as shaping various layers of the global techno-political landscape. My position departs from conventional wisdom about why donors provide capacity building assistance in the context of digital development, which has pointed to either (technical) cybersecurity or developmental goals. Rather, I contend that there is a third logic centered around networked, geostrategic competition which may motivate state-based donors' provision(s) of capacity building assistance.

To examine the intuition underlying the argument, the article undertakes a plausibility probe of Chinese, EU, and US provisions of capacity building assistance for digital development on the African continent. Qualitative analyses of primary source documents, interviews, and secondary sources reveals that donors have advanced a geostrategic, competitive rationale for incorporating 'cybersecurity' and 'digital' capacity building assistance into broader digital development programs. Further, EU, US, and Chinese provisions of capacity building assistance appear to have been mediated by the following donor strategies: *conditionality, restriction,* and *targeted empowerment*. In this context, I discuss how variation in donors' provision of capacity building assistance appears to have been shaped by three important factors: the donor's relative access to and control over the intermediary provider, their normative approach to development, and the locus of geopolitical competition.

This study makes several distinct contributions to IR literature, contemporary security studies and cybersecurity scholarship. First, it supplements gaps in nascent cyber-IR literature by theorizing how capacity building assistance, as a foreign policy instrument, has been shaped by donors' perceptions of strategic advantage. Second, the article engages weaponized interdependence scholarship through a novel angle by exploring the context of capacity building assistance and the various ways it can be perceived by donors as enabling them to leverage relations of digital interdependence. Finally, the article seeks to contribute to our understanding of the evolving relationship between geopolitical competition, digital cooperation, and networked interdependence (e.g. Sukumar et al., 2024; Pohle & Voelsen, 2022). Exploring this phenomenon is crucial in the context of rising global demand for cyber and digital capacity *and* escalating strategic competition between the People's Republic of China (PRC), the EU and the US.

In what follows, I review how extant scholarship has explained donors' provisions of capacity building assistance for digital development and the tensions it raises for the article's research questions. Next, I lay out the theoretical argument and methodology, followed by a two-step empirical analysis of US, Chinese, and EU provisions of capacity building assistance for digital development in Africa. Finally, I discusses these findings as they relate to the paper's research agenda and I offer several preliminary conclusions.

Providing capacity building assistance for digital development: rationales and tensions

This article interrogates the strategic dimension to capacity building assistance for digital development, whereby assistance is provided by a foreign state-based donor to a recipient. In this section, I review common debates on this subject and I argue that they have failed to adequately conceptualize and explain recent patterns in digital development assistance. In brief, both the cybersecurity and development literatures on capacity building assistance have tended to adopt siloed approaches to capacity building assistance as a component of digital development. These approaches are challenged by a global demand for integrating 'cyber' and 'digital' policy issues by the foreign and development policy communities, conceptual overlap between 'cyber' and 'digital' capacity building, and recent insights by scholarship on digital development and weaponized interdependence. Such changes beg for further theorization about the strategic import of capacity building assistance for powerful state-based donors—beyond conventional explanations premised upon technical cybersecurity and/or development goals.

Extant literature on capacity building in the context of digital development has tended to adopt a siloed approach to 'cyber' or 'digital' capacity tools. Historically, 'digital capacity building' instruments have been associated with traditional development objectives, sometimes eschewing the language of 'security' due to its perceived incompatibility with

developmental goals (Hathaway & Spidalieri, 2021, p. 29). By contrast, 'cyber capacity building' has been normally siloed to matters of technical cybersecurity, separable in theory and practice from digital development (Hathaway & Spidalieri, 2021, p. 29-30).

Mirroring this divide, two dominant explanations have been advanced to explain why donors provide capacity building assistance for digital development from a strategic perspective. On the one hand, scholars have emphasized the importance of capacity building assistance for development-oriented and/or normative reasons. By this account, capacity building for digital development, often termed '*digital* capacity building', has been associated with developmental progress, humanitarian values, and the UN Sustainable Development Goals (Collett, 2021). However, scholars have also argued that capacity building initiatives can serve to promulgate a donor's preferred cyber norms to recipients (Homburger, 2019; Hurel, 2022) and ensure a donor's preferential access to institutions via bilateral channels and/or socialization processes (Renard, 2018).

On the other hand, cybersecurity literature has stressed the potential for '*cyber* capacity building' to build recipients' resilience to (cyber)security risks, including to weaponized (digital) interdependence (Christou, 2016; Collett, 2021). Scholars have suggested that states with weak capabilities to detect or respond to cyber threats, high dependence upon a single vendor (Kaska et al., 2019), low governance capacity, and/or weak protections over critical national infrastructure (CNI) could be especially vulnerable to subversion and espionage (Maschmeyer, 2023), thus exacerbating potential insecurities in global cyberspace (Pawlak, 2016; Homburger, 2019). Therefore, from a technical security perspective, improving the cyber resilience of one vulnerable state—for example, by building scalable, secure, and redundant connectivity infrastructure—could increase the security of the wider network of connected states (Kaska et al., 2019; Tiirmaa-Klaar, 2016). Overall, this perspective suggests that there is an incentive for the donor to build the cyber

capacity of other states to avoid the negative spillover effects of incapable/insecure states on their domestic security and/or global stability (Oppenheimer, 2023; Lopez, 2023; Pawlak, 2016).

Contemporary approaches towards capacity building for digital development expose considerable gaps in the explanatory leverage of the above accounts. Foremost, while cyber and digital capacity building assistance may each possess broadly identifiable characteristics across policy communities (see Appendix A), there is no universally agreed-upon distinction between the two concepts in theory or practice (Hurel, 2022; Hathaway & Spidalieri, 2021). Rather, scholars have recently recognized that the concepts of 'digital' and 'cyber' capacity building are inherently subjective (Hurel, 2022), and their distinctive meanings vary across different policy contexts (Hathaway & Spidalieri, 2021; Collett & Barmpaliou, 2021) and over time (for the case of the EU, see Carver, 2024, pp. 2267-69). Recently, when state and non-state actors have distinguished between 'cyber' and 'digital' capacity, it has often been to demand their further *integration* in the context of digital development assistance (Pawlak & Barmpaliou, 2023; Hathaway & Spidalieri, 2021; GCSCC, n.d). This discursive reality undermines categorical assumptions about 'cyber' and 'digital' capacity building as entailing distinct (and sometimes competing) strategic rationales.

Convergence between digital and cyber capacity building tools in practice have been driven both by key international actors in the cybersecurity and development communities (e.g. Hathaway & Spidalieri, 2021; Hameed et al., 2018) and states' growing recognition that 'cyber' should be considered an enabler of digital transformation (Carver, 2024). Indeed, in multilateral and bilateral fora, donors have widely framed their digital infrastructure investments as building *both* the cybersecurity and digital capacities of recipients by providing (secure) critical national infrastructure and further digitalization (Hathaway & Spidalieri, 2021; see also UNIDIR, 2024; UN GGE, 2015, p. 11). Given that 'digital' and

'cyber' capacity building issues have increasingly become blurry and often overlapping concepts in practice (Collett & Barmpaliou, 2021; see also Aiken & Kumar 2019, p.1), it is reasonable to question whether siloed cybersecurity/digital development explanations can sufficiently grasp the complexity of capacity building assistance and account for donors' perceptions of its strategic import.

Moreover, both cybersecurity and development-based strands of explanations have struggled to provide sufficient explanations for recent global patterns of digital development assistance. Following the technical cybersecurity-based argument, one would expect provisions of capacity building assistance to target the 'weakest links' in the cyber ecosystem, for example by identifying and prioritizing the key spillover risks, network chokepoints and/or outstanding vulnerabilities. However, cyber capacity building tools and partnerships have been criticized as supply-driven (Hurel, 2022; Hathaway & Spidalieri, 2021) and as reproducing the "darling" phenomenon, whereby a small group of African 'darling' countries have been lavished by investments at the exclusion of others (Pawlak & Barmpaliou, 2017; see also Tugendhat & Voo, 2021; Munga & Monye, 2024).

While development-oriented explanations are better placed to explain the 'darling' phenomenon of capacity building investments than technical cybersecurity-oriented accounts, both approaches have failed to elaborate how strategic competition, such as geopolitical pressures, could shape such assistance. While some scholars have equivocated this possibility (e.g. Homburger, 2019; Hathaway & Spidalieri, 2021; see also Bermeo, 2018, pp. 145-150) it has not been examined in depth by extant literature. Yet, if capacity building assistance for digital development serves higher-level diplomatic and normative objectives "as a strategic tool of foreign policy" (Pawlak, 2016, p. 83), donors may well be motivated by geostrategic goals, particularly given the growing significance of digital sovereignty issues for geopolitical competition (Seidl, 2024). Ultimately, as Edmunds and Juncos put it,

"much of the [international relations] work which touches on capacity building not only fails to conceptualise this term, but also to theorise the power relations which sustain these practices, both at the domestic and international level" (2019, p. 5).

Moreover, both cybersecurity and development-oriented accounts come into tension with burgeoning literature on the relationship between digital development practices and weaponized interdependence risks (e.g. Narlikar, 2021). Rather than emphasizing the potential gains of providing assistance, this literature suggests that, under certain conditions, there are strategic incentives for powerful donors to *withhold* assistance, particularly if these actors can leverage their position in an asymmetric interdependent relationship (Drezner et al., 2021; Farrell & Newman, 2019). In the context of digital development, this conversation has overlapped with worries about the potential geopolitical and neocolonial motives to China's BRI (Hall & Krolikowski, 2022). This will be elaborated in the next section of the paper.

Altogether, these literatures presuppose alternate rationales underlying how donors may perceive capacity building provisions for digital development as shaping their strategic advantage. The gaps and tensions in these approaches impel further theorizing about the strategic value of capacity building assistance for digital development and its potential relationship to geopolitical competition. The next section addresses this lacuna by theorizing how, if at all, donors could perceive capacity building assistance for digital development as a means of engaging in geostrategic competition.

Beyond security and development: digital and cyber capacity building for strategic competition

How, then, do powerful state-based donors perceive capacity building assistance for digital development as shaping their strategic advantage? Further, which factors have shaped variation in donors' provision of such capacity building assistance to developing states?

Drawing upon insights from scholarship on networked power, weaponized interdependence, and traditional (military) security assistance, I theorize that donors perceive capacity assistance for digital development as a form of competitive strategic alignment. Specifically, I argue that state-based donors may not only perceive such assistance as offering developmental and/or cybersecurity dividends but also *potential strategic gains*.

Secondly, I theorize that donors can calibrate their capacity building assistance with three distinct practices—*conditionality*, *restriction*, and *targeted empowerment*—in line with their perceptions about capacity building as a tool for networked competition. In this regard, I contend that donors' relative access to and control over the intermediary provider of assistance (e.g. a private contractor), the donor's normative approach to development, and the locus of geopolitical competition are theorized to mediate the provision of capacity building assistance.

Perceptions of strategic advantage: Capacity building as shaping digital networked competition

To theorize how donors perceive capacity building assistance for digital development as a strategic tool, I draw from the literatures on networked power and (weaponized) interdependence. By foregrounding actors' attempts to "exercise power within and over networks" (Pohle & Voelsen, 2022, p. 14), networked-based scholarship provides useful analytical tools to theorize the relationship between powerful (state-based) donors' provision of capacity building assistance and their perceived strategic gains. This framing is appropriate given that capacity building assistance characterized by interdependent and asymmetric donor-recipient relationships (Hurel, 2022, p. 79; see also Baran, 2022, p. 748). Moreover, a network-based approach accounts for the reality that the digital environment is characterized by an asymmetric, networked digital architecture—from its physical backbone (Gjesvik, 2023) to its virtual and human layers—further highlighting an imbalanced power

dynamic between donors and recipients of digital development assistance. Indeed, scholars have argued that the techno-political reconfiguration of the internet has broadly offered opportunities for powerful actors "to subordinate particular subnetworks to a more centralised logic (power *over* networks)" and, "at the same time, expand and institutionalise their power position within these networks (power *within* networks)" (Pohle & Voelsen, 2022, p. 15-16; see also Farrell & Newman, 2019; Drezner et al., 2021; Hafner-Burton et al., 2009; Zajacz, 2019).

Through this lens, capacity building assistance for digital development can be conceived as potentially increasing the donor's power over and within the global digital network through the formation of greater social and/or structural ties. By pursuing such partnerships at scale, donors can pursue a more centralized position *within* the network through various pathways: for instance, by shaping outcomes at the country level (e.g. by influencing the country's legislative, security, or commercial environment), influencing regional institutions (e.g. joint collaborations on cybersecurity best practices), or by mobilizing these partnerships in the context of global institutions (e.g. by promoting their own approach as global norms). Here, power *within* the network may coincide with power *over* the network (Pohle & Voelsen, 2022). For example, by providing infrastructural assistance and technologies, donors can develop parts of the network in line with their routing preferences whilst shaping the technical standards for the technology's implementation (see also Gjesvik, 2023; Tugendhat, 2021) and potentially maintaining privileged access to the ICT infrastructure itself (see also Denis, 2021; Farrell & Newman, 2019). However, scholars have argued that to leverage asymmetric power over the network, an actor (e.g. donor) must have the institutional capacity to exercise territorial or jurisdictional claims over the hub in the network, including private firms (Farrell & Newman, 2019). From this perspective, strategic competition through networks is shaped

by the structural features of the global digital domain, relations of interdependence, and a state's domestic characteristics.

Consequently, by potentially reshaping social, normative, and structural ties with recipients (and thereby wider parts of the digital network), capacity building assistance could contribute to the balancing or hedging strategies of powerful donors. Outside of the cybersecurity and digital politics literatures, scholars have argued that providing security assistance to prospective partners can be part of an external balancing (Tecott Metz, 2023; Meijer & Simón, 2021), shaping (Wolfley, 2022), or wedge strategy (Huang, 2020). I suggest here that a similar logic could apply; by providing training, governance initiatives and structural investments, the donor may perceive an opportunity to (re)shape the recipient's standards, norms, and/or technological relationships to better support the donor's strategic objectives.

Tailoring capacity building assistance strategies

Assuming that donors may perceive capacity building assistance as a form of networked, strategic alignment, they would arguably have a strong incentive to calibrate their provisions of assistance to sustain a preferable alignment with recipients (and reduce potential sunk costs). On this basis, I argue that donors may seek to calibrate their assistance in line with three broad practices (or strategies): *conditionality, restriction*, and *targeted empowerment*. Whereas the first two practices encourage the recipient's closer alignment to the donor, targeted empowerment incorporates aims to drive a "wedge" between the recipient and a prospective rival donor as another strategy of competition.

Attaching *conditionality* instruments to capacity building provisions encourages sustained alignment with the donor by stipulating the recipient's alignment to favorable institutions, practices, and standards. A strategy of conditionality may also be preferred on

account of the donor's normative approach to development. For example, Western assistance is often characterized by a requirement for the recipient to emulate or uphold commitments to certain values or rights, which constitute "conditions" for the investment (see also Prontera & Quintzow, 2022). Thus, rather than exerting direct structural control or access over a recipient's infrastructure, conditionality can be understood as a form of regulatory control by shaping the recipient's standards and rules in line with donor preferences (see also Cortela, 2007). Accordingly, such a strategy is conducive to the transfer of substantive skills, technologies, and norms (to help the recipient fulfil conditionality), including cybersecurity skills and digital vocational training.

By contrast, donors may enjoy a higher degree of access or control over key aspects of the recipient's digital infrastructure (e.g. through the ownership of a monopolistic ICT firm in a recipient state), enabling increased structural control over the cooperative relationship (Drezner, et al., 2021; Park & Tang, 2021; Tugendhat, 2021). Here, a strategy of *restriction* might be preferred under permissible normative conditions. This strategy maintains a relational asymmetry between the donor and recipient through restricting access to key knowledge, thus placing the recipient in a position of sustained dependency on the donor for its capacity to operate and maintain domestic services. Examples of restriction include 1) withholding substantive knowledge surrounding the management or operation of technology (or the sector) in favor of small-scale skills transfers and 2) requiring the presence of a foreign (donor-based) contractor in the provision of local services to maintain control. Here, the capacity building provision policy could be framed as "no strings attached"—an attractive alternative to conditional assistance (see also Baran, 2022, p. 747). Nonetheless, the donor restricts access to knowledge and opportunities which could have further enabled the recipient's indigeneity.

Finally, capacity building assistance can be leveraged to drive a wedge between a recipient and another donor by offsetting a rival's assistance (see also Blair et al., 2022, p. 1360). For instance, if a rival donor is undertaking a strategy of restriction with a recipient, another competitor could focus on building up the recipient's substantive skills through knowledge transfers, such as cybersecurity skills training, thus addressing the capacity gaps and nullifying the effects of restriction. Conversely, the competing donor might broker a deal with the recipient on a different dimension of digital cooperation on a "no strings attached" policy, thus skirting the conditionality requirements of the rival (see also Dreher et al., 2022). For example, China has spurned conditionality measures in its provision of development financing in part to compete with American and European investment programs (Blair et al., 2022). Thus, conditionality instruments or 'no string attached' approaches may also be calibrated to offset the recipient's alignment with a competing donor.

Altogether, assuming that powerful state-based donors perceive capacity building as a means to engage in networked competition, I expect that their provision of capacity building assistance tools is shaped by three important factors: their relative access to and control over the intermediary provider of assistance (e.g. a private and/or company contractor), the donor's normative approach to development, and the locus of geopolitical competition (competitive pressures). Given prior EU and US engagement with conditionality instruments, their lack of direct control over private intermediaries, and their liberal democratic principles, I would expect that these donors would engage with conditionality instruments in their provision of capacity building assistance for digital development in Africa (see also Blauberger & Van Hüllen, 2021; Cortela, 2007; Prontera & Quintzow, 2022). Conversely, by virtue of the PRC's reportedly closer oversight and ownership over the intermediaries tasked with development assistance (Park & Tang, 2021;

Schwarz & Rudyak, 2023, p. 29-30; Tugendhat, 2021, cf. Kernen & Lam, 2014), as well as the Chinese government's track record of providing "no strings attached" infrastructural assistance to African states (Dreher et al., 2022; Blair et al., 2022), I would expect Chinese provisions to be compatible with a strategy of restriction. This variation also underscores the normative component to capacity building programs: such assistance is tailored by the donor's values and political orientation towards development (Collett & Barmpaliou, 2021). Finally, I would expect all three donors to pursue capacity building projects competitively, targeting their assistance in ways which enable them to compete with other donors and shape the broader geopolitical environment. Table 4.5 below summarizes these theoretical expectations and provides broad empirical indicators for each practice.

Three capacity building calibration practices and empirical indicators	
Strategy	**Indicators**
Conditionality	Conditions attached to the provision of assistance and/or funding for capacity building. Donations of training, infrastructure assistance, and sharing of best practices may also be tailored by the donor to enable the recipient to fulfil conditionality requirements.
Restriction	Provisions of skills transfers are selective, not generalizable, or independently sustainable without foreign assistance, leading to operational or technical dependency on the donor. Also evidenced by a recipient's formal reliance on an external contractor for the knowledge, sustainability, and maintenance of digital infrastructure or cybersecurity technologies in their local sectors (e.g. contractually requiring the presence of a foreign, donor-based operator or vendor in the provision of a local service).
Targeted empowerment	Pursuing a competitive advantage within a particular developmental context against another donor, e.g. by offsetting a rival's assistance through complementary and/or competing policy tools and interventions. Observable geopolitical, competitive logic in policy documents as the rationale for assistance, as well as presence of multiple competing projects in one policy area/region/context.
Table 4.5. Theorized donor strategies for calibrating assistance and empirical indicators.	

Methodology

To probe the plausibility of my argument and theoretical expectations, I examined US, EU and Chinese provisions in the context of African states' digital development. The article's empirical analysis comprised two steps. First, I conducted a discourse analysis of Chinese, EU, and US primary sources (detailed below) to explore donor perceptions about the strategic import of capacity building to understand which strategic objectives, rationales, and problems are articulated by these three actors as motivating their provisions of capacity building assistance for African states' digital development.

Second, to identify variation in the three donors' approaches to providing capacity building assistance, I focused upon three levels of intervention relevant to digital development: 1) (digital) infrastructural assistance; 2) knowledge transfers at the sectoral level; 3) norms transfers at the governance level. These three dimensions were selected after mapping extant literature (refer to Appendix A; see also Homburger, 2019; UN GGE, p.11, 2015) with the stated policy priorities of the US, China, and the EU, including how these donors have conceptualized 'capacity building' in the context of digital development, as such conceptualizations are subjective (as previously reviewed). Within these levels of analysis, I identified relevant African state recipients of EU, US, and Chinese practices in line with available data. I then corroborated these aspects by conducting interviews with key policy stakeholders and with existing empirical evidence of African digital development projects.

Accordingly, my interpretive-qualitative discourse analysis leveraged both primary and secondary textual sources (Schwartz-Shea & Yanow, 2012). Textual findings were corroborated by five Europe-based formal elite interviews that I conducted over 2021-2022 and three UK and US-based informal interviews in 2024 (see Appendix B). Primary source documents included foreign policy strategies, executive orders, speeches, diplomatic

statements and communiqués, intergovernmental reports (e.g from the UN), staff working documents (SWDs), white papers, and memos. In terms of secondary sources, I leveraged English translations of Chinese documents, NGO reports (e.g. from the OECD, and the GFCE), ethnographic research, and academic databases about Chinese development investments (e.g. Makundi et al., 2016; Park & Tang, 2021; Dreher et al., 2021; Agbebi, 2018; Chinese Loans to Africa database, 2023).

The diverse corpus of data enabled me to survey various policy contexts, including official statements on the significance of capacity building assistance and internal-facing documents, including SWDs and project guidelines, from an operational perspective. Qualitative data were analyzed with attention to 1) how different actors have framed capacity building assistance as addressing particular policy "problems" (Bacchi & Goodwin, 2016); and 2) the rationale for selecting particular forms of capacity building assistance tools, including their perceived impact from the perspectives of donor and recipient. I also drew upon this corpus to probe for the presence of the assistance strategies theorized in my analytical framework (viz. conditionality, restriction, and targeted empowerment) across the three levels of policy intervention outlined above.

In line with the article's primary research question on donor perceptions, my analytical approach is predominantly focused upon the supply side of digital development assistance, particularly EU, US, and Chinese assistance to African states. By and large, capacity building assistance has remained supply driven and export-oriented, often failing to account for the specific technical needs of recipient countries, even in the context of the 'participatory turn' of Western development assistance (Hathaway & Spidalieri, 2021; Hurel, 2022; see also Edmunds & Juncos, 2019, p. 4; Baran, 2022, p. 746-7). This reality underscores the importance of examining how donors conceive of capacity building

initiatives in digital development and their integration into broader strategic goals—and not only donations from the so-called Global North, but also the Global South (e.g. Chinese provisions).

Given the above approach, this article does not seek to advance a universal theory about all contexts and actors involved in capacity building for digital development. However, it does aim to produce insights about EU, US, and Chinese approaches to capacity building assistance in the cases of several African states explored by the analysis, as a valuable point of departure for future research and inference about the significance of capacity building for digital development as a tool of strategic advantage. Below, I explain how the context of US, EU, and Chinese digital development assistance directed towards African states offers a fruitful empirical basis for examining how, if at all, powerful state-based donors perceive capacity building assistance for digital development as shaping their strategic advantage.

Digital development cooperation in Africa as the site of US-EU-China geostrategic competition

With the most rapidly expanding telecommunications market in the world, Africa hosts high demand for capacity building in the context of digital development (Ramim & Hueca, 2021). Beijing, Brussels, and Washington—all major trade partners to African countries—have responded to this demand by providing some of the highest amounts of digital development assistance to African countries in the world (UNCTAD, 2019). Given that the African continent has received the highest amount of bilateral (official) development funds for digitalisation (37.9%) in the world, the scale of US, EU, and Chinese financing is significant (Gualberti & Wicks, 2021). Concurrently, funding for cyber capacity building in Africa has increased over time, albeit unequally: out of the cyber capacity building projects

involving African Union members, 25% are based in five countries: Kenya, Ghana, Nigeria, Botswana, and Rwanda (Collett & Barmpaliou, 2021).

The sheer scale of US, EU, and Chinese contributions to Africa's digital development is partly captured by the budgets of their major digital development initiatives. In 2022, Washington announced the *Digital Transformation with Africa* (DTA) initiative, investing over USD $350 million (and an additional $450 million in finance facilitation) to address Africa's digital economy and infrastructure, human capital development, and provide a digital enabling environment (US Department of State, n.d.). Seeking to target all African countries, the DTA has already invested USD $82 million in its first year of implementation (Munga & Monye, 2024). Reflecting some aspects of DTA funding, the US government's annual spending on cyber capacity building has quintupled since 2017 (Collett & Barmpaliou, 2021).

Separately, China is estimated to provide USD $13.2 billion in ICT loans to Africa (Chinese Loans to Africa database, 2023), and at least sixteen African countries have reportedly signed cooperation agreements with China's "Digital Silk Road" digital investment framework as part of Beijing's colossal BRI (Feldstein, 2020).

Meanwhile, the EU's provision of cyber capacity building assistance has become more integrated with digital development under the von der Leyen Commission (Carver, 2024; General Secretariat of the Council, 2021). Through the framework of the €300 billion *Global Gateway* connectivity project—the EU's alternative to the BRI (Haroche, 2022)—the EU has invested €8 billion to facilitate an AU-EU Digital for Development Hub and €4.89 billion on digital innovation in Africa (European Commission, n.d.; 2022b). The EU also sources financing through its "Team Europe" approach (drawing upon states' development finance and program partners) and it has announced plans to invest in €430

million in a Digital Economy Partnership with Kenya (European Commission, 2023) and €820 million in a similar partnership with Nigeria (European Union, 2022).

These investments are notable given recent academic speculation that the EU, US, and China could emerge as three main "hubs" of the digital domain, which would enable them to leverage their central positions and control over global digital networks for strategic advantage (Farrell & Newman, 2019). Domestically and abroad, Beijing has retained tight control over multinational Chinese firms through different mechanisms, including national security legislation, centralization efforts, and state ownership (Kokas, 2022, cf. Kernen & Lam, 2014). On the other hand, the US and the EU have less direct control over private firms. Nonetheless, they have each established close partnerships with corporations and businesses for investing in digital development through a variety of (domestic) governmental or multistakeholder arrangements. Under the Biden Administration, Washington has reformed its traditional financing approach to increase the role of private capital in state development finance (White House, 2021). Moreover, the EU has demonstrated considerable regulatory power over firms through a variety of stringent legal constraints on data privacy, including its GDPR law (Kuner, 2019). Furthermore, China, the EU, and the US have each been accused of already engaging in practices of weaponizing interdependence in other policy domains. Most notoriously, in 2018, China was accused of conducting years of cyber espionage and data exfiltration against the African Union by exploiting the very ICT infrastructure it had previously "gifted' to the AU build the Union's capacity (Kadiri et al., 2018).

Overall, Africa's digital development landscape reveals the *opportunities* for powerful actors to engage in geopolitical competition. However, for my theoretical framework to hold, there should also exist observable supply-side geopolitical competition

between donors, donors' awareness that global (digital) networks can be leveraged for strategic advantage, and their willingness to engage in networked competition. Indeed, as I argue below, the African digital development context reveals that the EU, US, and China are currently engaged in competitive strategic relations in the digital domain. These powerful global actors are not only capable pursuing strategic gains through global digital networks, but they have recognized asymmetric interdependence as a form of strategic advantage in the digital domain.

Strategic perceptions: the EU, US, and China as engaging in networked competition through digital development

Documentary evidence and interviews reveal that digital development cooperation and capacity building partnerships have become strategically important for Brussels, Washington, and Beijing to promote their interests globally. In this vein, US, EU, and Chinese foreign policy discourses have also constructed digital and cyber capacity (development) gaps as constituting vulnerabilities to networked influence and great power competition—often implicating their strategic competitors for engaging in such behavior.

Strategic competition through digital development and technological alliances

In 2021, the EU's *Digital Compass,* a broad strategic document for the Union's Digital Decade, highlighted that "the…digitalisation of an economy or society has been shown not only to be a critical underpinning of economic and societal resilience, but also a factor in global influence" (European Commission, 2021b). The *Compass* outlined how "The EU's international digital partnerships will be underpinned by a toolbox, drawing on a combination of regulatory cooperation*,* addressing capacity building and skills, investment in international cooperation and research partnerships" (European Commission, 2021b). This multifaceted approach is important, as the EU's High Representative, Josep Borrell declared in 2020, "We live in a world where interdependence is becoming more and more

conflictual and where soft power is weaponised: trade, technology, data, information are now instruments of political competition" (European External Action Service, 2020; see also Lopez, 2023).

Building upon the *Digital Compass,* Brussels has acknowledged that China's rising involvement in global development has served as the "prime motivator" for the EU's new €300 billion *Global Gateway* connectivity project (Interviewee 5; Pawlak & Barmpaliou, 2023; Erforth & Fritzsche, 2022). The Global Gateway is aimed at promoting the "European model of trusted connectivity' in the areas of digital, climate and energy, transport, health, education and research" (European Commission, 2021a). The European Commission has described its Global Gateway investment program as, *"reaffirming our vision of boosting a network of connections*, which must be based on internationally accepted standards, rules and regulations in order to provide a level-playing field" (emphasis added by author, 2021a). Notably, EU officials have contrasted the EU's capacity building and development ethos with Russian and Chinese approaches, which are seen as creating digital dependencies and a *lack* of a level playing field (Interviewee 1).

Separately, geopolitical positioning, digital dependence, and networked influence are currently represented by US government documents as key issues for digital development (USAID, 2023; n.d). USAID's *Digital Ecosystem Country Assessments* (DECA) initiative, a flagship of Washington's current *Digital Strategy*, has stressed "geopolitical positioning" and "cybersecurity" as two "cross-cutting topics" which must be considered for all areas of DECA, given that the digital environment is composed of "innately interdependent [elements]," (USAID, n.d.). Accordingly, investing in Africa's digital transformation is crucial for Washington because "Africa is a major geopolitical force" (Secretary of State Anthony Blinken, quoted in United States Department of State, 2023).

Discursive links between geostrategic competition, global digital partnerships, and strategic advantage are further exemplified in the current US *Defense Strategy* (2023), which makes the following statement about the PRC:

> 'The PRC seeks advantages in cyberspace in order to facilitate its emergence as a superpower with commensurate political, military, and economic influence. By exercising effective state control over businesses with large market share in the telecommunications, commercial hardware and software, and cybersecurity industries, the PRC tries to shape the global technology ecosystem. It exports dangerous cyber capabilities to like-minded nations and works to accelerate the rise of digital authoritarianism around the globe (p. 4).'

With a strikingly similar framing to its geopolitical competitor, the Chinese Ministry of Foreign Affairs published an English statement on *US Hegemony and its Perils* in February 2023. The statement outlined the various ways in which Washington "abuses its hegemony," including through "digital alliances" (2023). The Ministry went on to accuse the US of "politiciz[ing] and weaponiz[ing] technological issues" by "mobilizing state power" to "suppress" the Chinese state-owned company Huawei from entering its market, and "coerc[ing] other countries to ban Huawei from undertaking local 5G network construction." Several months later, the Ministry released another acrimonious statement on US foreign aid, asserting that: "At present, U.S. not only unabashedly proclaims its self-serving intention to provide foreign aid, but also pushes aid to the main battlefield of great power games" (Chinese Ministry of Foreign Affairs, 2024). Unsurprisingly, then, Beijing has competitively positioned its own investment packages with African partners as "no strings attached" and offering "win-win" alternatives to the Western approach (China Daily, 2018; see also Ministry of Foreign Affairs of the People's Republic of China, 2024).

Consequently, US, EU, and Chinese digital development policies towards Africa must be understood within the broader context of geopolitical competition and digital interdependence. Becoming increasingly rivalrous, Sino-American competition has spilled

over to a multitude of policy areas such as technology, industrial policy, diplomacy, and development (European External Action Service, 2020). In 2018, the US administration "updated [the US] China policy to bring the concept of competition to the forefront" (in Zhao, 2019, p. 372), and the government labelled China a "strategic competitor" in the 2023 US *National Defense Strategy*. Separately, the EU has labelled Beijing an "economic competitor" and "systemic rival" (European External Action Service, 2022), and Brussels stated its ambitions to become an unequivocally "geopolitical actor" in 2020 (Von der Leyen, 2020; see also Haroche, 2022).

Furthermore, while Brussels and Washington do not perceive each other as systemic geopolitical rivals, they compete over a variety of global digital policy issues, including data governance (Pawlak & Barmpaliou, 2023). Caught between US-China competition (Weber, 2020), the EU has articulated a desire to distinguish itself from Washington and articulate its own approach to sovereignty in the digital domain as part of its "geopolitical Commission," (Barrinha & Christou, 2022). In turn, Washington has sought to distinguish its "digital solidarity" approach from the aims of the EU's "digital sovereignty" agenda (US Department of State, 2024). Thus, whereas Brussels' approach to digital development promotes "made in Europe" solutions in its capacity building projects (Pawlak, 2016; European Commission, 2022), Washington has sought to promote "American approaches" to cybersecurity through various aid and investment projects (USAID, 2020).

Declaring the significance of capacity building

Within this context, all three donors have publicly declared capacity building assistance as strategically important for their foreign policy goals, including vis-à-vis international security, leadership, and global competition. As US Secretary of State Blinken wrote,

> '…[W]e have prioritized building capacity and expertise in cyber, digital, and emerging technology issues as part of our broader efforts to modernize diplomacy and ensure U.S. foreign policy delivers on the issues that matter most to the lives and livelihoods of the American people (quoted in US State Department, 2024).'

Consequently, the US' new strategic approach to cyberspace and digital technologies is underpinned by the idea of "digital solidarity", defined as "a willingness to work together on shared goals, to help partners build capacity, and to provide mutual support" (US Department of State, 2024). Notably, the government also recognized that, "Adversaries, and the PRC in particular […] look to *out-match the United States* and like-minded partners by offering holistic support for ICT development from full package training programs to higher-level education and scholarships" (emphasis added by author, US Department of State, 2024).

China, too, has recently placed greater discursive emphasis on cyber and digital capacity building for its strategic goals, including in collaboration with the African Union (Ministry of Foreign Affairs of the People's Republic of China, 2017; Ren, 2019). This turn was foreshadowed by President Xi's 2015 UN speech about the importance of capacity building for development and "South-South Cooperation." The Xi government has also conceived of development "primarily as a process of technology-centered modernization" (Rudyak, 2021, in Rudyak & Schwarz, 2023, p. 15, see also Ministry of Foreign Affairs for the People's Republic of China, 2016).

Likewise, in the EU context, external capacity building has been touted as a key pillar in its foreign policy (General Secretariat of the Council, 2018), a "strategic building block" for its cyber diplomacy efforts (Council of the EU Presidency, 2016), and a means to embed "Made in Europe solutions" overseas (Pawlak, 2018; see also Pawlak & Barmpaliou, 2023, p. 13). As suggested by statements in the EU's *Digital Compass,* capacity building for digital

development has increasingly been mainstreamed into the EU's broader external action goals (European Commission, 2021b; Carver, 2024). How these donors have engaged with capacity building assistance in the context of Africa's digital development is explored below.

Donor investments across three levels of capacity building assistance for Africa's digital development

The ensuing analysis reveals patterns of donor competition over Africa's digital development which support the article's theoretical arguments about capacity building assistance as a perceived tool of strategic alignment for donors. These patterns are evidenced across three common levels of capacity building interventions: infrastructural support and funding, sectoral skills, and governance/regulation.

The infrastructure level: "No strings attached" vs. capacity building as an inducement

The past decade has seen heightened competition between the US, China, and the EU over providing cybersecurity and digital-oriented infrastructural assistance to African states. Particularly, donors' financing of internet connectivity (including fibreoptic cables) constitutes a rapidly growing sector for Africa's digital transformation and an emerging area of geopolitical competition (Erforth & Fritzsche, 2021). While early parts of the "internet backbone" were primarily owned by the US and its partners—and scarcely reached the African continent—the "second undersea cable boom" in 2015 ushered in new opportunities to challenge US centrality over the global internet backbone through constructing alternate cable routes and shaping their regulation (Gjesvik, 2023; McGeachy, 2022).

Over this period, China has been a first mover in developing Africa's internet backbone, from undersea cables to telecommunications infrastructure (Agbebi et al., 2021). Indeed, the Chinese state-sponsored multinational firm Huawei supplies components and infrastructure for approximately 70% of 4G networks across Africa and it has a leading

market position in 5G provisions (Ehl, 2022), including in Botswana and Tanzania (Agbebi, 2018). Additionally, Chinese multinational firms ZTE and Alibaba retain a dominant position in Africa's telecommunications market, edging out major Western firms such as Ericsson and Siemens (Agbebi, 2018). Notably, the PRC has consistently expressed its opposition to using conditionality instruments for its digital infrastructure investments (Zhang Jun, in Minlu, 2022).

President Xi's "no strings attached" approach is evidenced by the PRC's funding of global undersea cable ventures owned and/or developed by Chinese companies, such as the firm HMN Technologies (Hengtong Group). One such cable system, the PEACE Cable, asserts that it will "provide a cost-effective, diverse route for the escalating demand for capacity among Asia, Africa and Europe," (Peace Cable International Network Co., Ltd, 2018). The PEACE Cable System asserts that it guarantees a "Neutral Open System" with "no restrictions on participants" and "carrier-neutral" interconnections (PEACE Cable, n-d). This echoes President Xi Jinping's rhetoric of a "five-no" approach to development, which he expressed during the Forum on China–Africa Cooperation in 2018. This approach entails:

> '[…] No interference in African countries' pursuit of development paths that fit their national conditions; no interference in African countries' internal affairs; no imposition of our will on African countries; no attachment of political strings to assistance to Africa; and no seeking of selfish political gains in investment and financing cooperation with Africa (Xi Jinping, quoted in China Daily, 2018).'

This similarity is not surprising, given that HMN Technologies is known to have close ties with the Chinese government, recognized for their "civil-military integration" efforts with the PRC (Goodman & Wayland, 2022). Moreover, Hong Kong, the location of the PEACE Cable's landing base (and HMN Technologies), underwent strict changes to its national security law in 2020 which enabled Beijing to install a "vast security apparatus" in the

territory (Hernandez, 2021). It is also worth noting that HMN Technologies is a rebranded successor of Chinese company Huawei Marine, the fourth-largest manufacturer of undersea cables in the world (Submarine Cable Networks, n-d). The Cable's previous owner, the multinational firm Huawei, has been implicated in Beijing's alleged cyberespionage activities in African countries (Kokas, 2022; Ehl, 2022).

Whereas China has emerged as a dominant funder of African ICT infrastructure and technologies, both the EU and the US have lagged in their digital infrastructural investments. Recognizing China's first mover advantage, EU policymakers realized that the EU must "catch up" by establishing links with African partners, particularly in terms of infrastructural investment (Interviewees 1,4; Pawlak & Barmpaliou, 2023). Therefore, the "Digital" pillar of the EU's *Global Gateway Strategy* seeks to establish further infrastructural, industrial, and technological links with countries through various initiatives (European Commission, 2021a). In Africa, the EU has recently funded European satellite communications systems and fibre optic cable projects such as the "Africa Europe Digital Innovation Bridge" (AEDIB) and the EurAfrica Gateway Cable (European Commission, 2022a, 2022b).

The EU's approach to influence and competition through digital infrastructure financing departs from Beijing in two key areas: substantive skills training (including cyber capacity building) and conditionality instruments. The EU's Global Gateway entails investing in both "hard and soft infrastructure" to "build resilient connections with the world" (European Commission, 2021a). For example, according to EU investment documents, the EU's AEDIB project "will encourage bridging activities on technical capacity building and technology transfer between African and European innovators and start-ups, private sector actors, academia, local governments and investors," (European

Commission, 2022b). Brussels' "human-centric" approach (European Commission, n.d.-b) is evidenced further by analysis in the next two empirical sections.

Separately, the current Biden Administration has ramped up its investments for developing the digital infrastructure of emerging areas of the global digital network (White House, 2021; 2022), announcing its intention to "double down" on development finance for Africa (Perry & Menski, 2021). The White House's growing commitment to building Africa's digital infrastructure is further evidenced by its release of a *New Initiative on Digital Transformation with Africa (DTA*) in December 2022, whereby *Digital Economy and Infrastructure* is the first out of three core pillars (White House, 2022). The DTA initiative stresses a new "whole of government approach" which is poised to eclipse earlier US government efforts at building Africa's digital infrastructural capacity (White House, 2022). Alike the EU's Global Gateway, the DTA initiative exemplifies Washington's engagement with substantive capacity building tools in tandem with infrastructural investments. For example, in Ghana, US government agencies have claimed to provide 1) cybersecurity training to local companies in concert with Amazon Web Services and Cisco and 2) governmental representation to support Ghana's "global cyber capacity building efforts and the goals of the DTA" (US Embassy in Ghana, 2023).

Notwithstanding US and EU efforts to invest more in Africa's digital infrastructure, including in Botswana (US Embassy Gaborone, 2023) and Tanzania (USAID, 2023; European Union, 2022), they have been criticized as "grumbl[ing]" about Chinese investments "but compet[ing] less" in practice (The Economist, 2023). However, Washington's efforts to outcompete Chinese companies for stakes in global undersea cable projects illustrates how capacity building assistance has factored into its geostrategic approach to Beijing. Over the past four years, Washington has reportedly intervened in six

private undersea cable deals to preclude HMN Group from winning contracts or ensured "the rerouting or abandonment of cables that would have directly linked U.S. and Chinese territories" (Brock, 2023a). Indeed, a Reuters investigation found that the US government campaigned to halt HMN Group's awarding of the multimillion-dollar SeaMeWe-6 contract from 2020-23, using a combination of carrots and sticks (Brock, 2023a). Specifically, the USDTA reportedly offered training grants to local telecommunications companies situated on the prospective cable's route if they chose SubCom LLC (a US-based supplier) instead of HMN Group. At the same time, Washington applied coercive pressure, threatening sanctions on HMN Group through diplomatic meetings with the cable's partners and alleging that the Chinese company sought to "acquire American technology" to modernize the PLA (Alper & Psaledakis, 2021). Therefore, the US government has offered capacity building to local countries as an inducement for local countries to choose US connectivity providers over Chinese counterparts.

The sectoral level: Restriction vs. targeted empowerment

Building on the previous section, the US, EU, and China have adopted different approaches to knowledge transfers within the framework of larger digital development assistance projects. Due to their strong market presence in Africa's ICT sector, Chinese multinational firms such as Huawei, ZTE, and Alibaba are viewed as "well placed to contribute significantly to skill building and technology transfer" (Agbebi 2018, p. 532). Yet, studies have widely concluded that there has been *very little* substantive knowledge transferred from Chinese donors/contractors to African recipients (Park & Tang, 2021). Rather, evidence suggests that China's approach to knowledge transfers in Africa can heighten information asymmetries between Beijing and the recipients of its development projects—creating further dependencies between local actors and Beijing (e.g. Makundi et al., 2016).

Indeed, evidence of two major Chinese ICT providers in several African countries suggests the *restriction* of skills transfers at the sectoral level. The strategy of restriction is particularly apparent in case studies of Huawei's training activities in Africa. Huawei has invested considerably in training local employees, university students, and subcontractors, whether in the form of free University-level courses, training centres, or training "on the job" (Tugendhat, 2020). Despite ICT skills training serving as a "core plank" of its marketing strategy, Huawei's training provisions have been centred upon sharing information specific to its own products instead of general knowledge about the industry to local Africans (Tugendhat, 2020). Unlike its main (European-based) competitor, Cisco, Huawei is known to supply a principal engineer from its own staff to work with local partners, and it has been found to "cut out" local staff to close business with clients directly (Makundi et al., 2016). Thus, despite providing Africans with the capacity to sell and operate Huawei's own ICT technology, Huawei's strategy of excluding local partners from key industry decisions and contracts further reinforces the dominance of Huawei over the creation of African indigenous capacities. This generates further profits for the state-sponsored company at the expense of developing a competing indigenous capacity to provide similar services (Makundi et al., 2016).

Notably, restrictive approaches to knowledge transfer have also been practiced by the Chinese International Telecommunications Construction Corporation (CITCC), a Chinese state-owned company, in Tanzania. In this case, Makundi, Huyse and Develtere (2016) concluded that "the missing R&D and technology-advancing capabilities render Tanzania's dependency on China ongoing for advanced troubleshooting and technology upgrading" (p. 143). Tanzanian mobile network operators have also reported challenges with ensuring data security, as imported technology from China "has embedded software not accessible to local experts due to the language barrier, as some instructions are in Mandarin

Chinese" (USAID, 2023, p. 23). Other studies examining Chinese ICT companies (including ZTE) in Ghana have highlighted similar bottlenecks around local training and substantive technical skills transfers (Wang & Elliot, 2014 p. 1026; Kernen & Lam, 2014). Overall, the lack of cyber and digital capacity building transfers provided by Chinese state-sponsored firms has maintained overseas demand for Chinese technologies and expertise, thus sustaining dependencies on Chinese assets.

Meanwhile, the US and the EU have considered the building of "human" cyber capacity, (e.g. substantive knowledge transfers and skills training) as crucial to mitigating the vulnerabilities they associate with China's large ICT infrastructural footprint, particularly dependency risks (Denis, 2021; USAID, 2023). In this regard, EU and US provisions of substantive skills transfers for Tanzania's digital transformation can be understood as evincing the strategy of *targeted empowerment*.

As discussed above, Tanzania is the recipient of a variety of major ICT investments from China (paired with selective skills transfers and training). However, the Tanzanian government has also signed a memorandum of understanding with the US government's development bank, EXIM, to promote its digital transformation (White House, 2023), and it has partnered with the EU on the major EUR35 million program "Digital4Tanzania." In an internal document, the EU has explained the "Intervention Logic" for providing digital development assistance to Tanzania (including cyber and digital capacity building) as follows:

> 'The Action intends to contribute to the transformative impact digitalisation can bring to the socio-economic environment of Tanzania, both Mainland and Zanzibar…*There is an opportunity for the EU to position itself as an alternative partners [sic] to big players such as US and China* and promote EU values (e.g. on cybersecurity and data protection) and interests (e.g. promotion of EU digital investments in the country). (Emphasis added by author, European Union, 2021).'

In Tanzania and other AU countries, including Benin, Kenya, and Rwanda, the AU-EU D4D Hub has organized multiple multistakeholder dialogues for digital actors to foster "debate and partnerships on a wide range of topics, such as connectivity, digital entrepreneurship, data governance, cybersecurity, data protection, online disinformation, and e-governance" (European Union, 2021; see also European Union, 2022). For EU practitioners, a key guiding concept for capacity building assistance partnerships is the "to train principle," which is the process of sharing the lessons Europe has learned with partner countries to help guide their development (Interviewee 1). However, as scholars have argued elsewhere, this 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" (Bialasiewicz, 2015; see also Edmunds & Juncos, 2019).

Separately, a USAID report emphasized the need to build Tanzania's "soft" digital and cyber capacity in recognition of the influential role of PRC on the country's national connectivity infrastructure and technologies (USAID, 2023; 2022, p. 24). Thus, Washington launched a bilateral "Partnership on 5G Security and Cyber Cooperation" with Tanzania "to build capacity and collaborate on 5G, cybersecurity, and related regulatory policies and frameworks" within the framework of a broader trade agreement (White House, 2023). As the US Ambassador to Tanzania put in a recent podcast interview, "In Tanzania, we're trying to model [the relationship with China] off of the direction that the President and the Secretary of State takes. That it's a great power competition," (quoted in Dizolele, 2024). In a different case, the government's webpage on *Prosper Africa* initiative highlighted how program funding enabled an African-American entrepreneur to "*edge out a Chinese competitor* for a [cybersecurity and ICT infrastructure] contract with the Government of Burkina Faso," (emphasis added by author, Prosper Africa, 2021).

More broadly, Washington has recently announced its intention to "elevate [US] development diplomacy" by "plac[ing] greater emphasis on *local capacity strengthening*, prioritizing partnerships with local actors to jointly improve the performance of local systems" (emphasis added by author, USAID, 2023, p. 30). At the sectoral level, Washington's approach to knowledge transfers is evidenced by the *Digital Connectivity and Cybersecurity Partnership* (DCCP) (USAID, 2022, p. 1). The DCCP partnership is responsible for carrying out the *Promoting American Approaches* to ICT Policy and Regulation project, which seeks to assist "partner countries establish dedicated policy support in the form of technical assistance, embedded experts, capacity-building, and training" (USAID, 2020).

According to US State Department (2024) estimates, 35 African countries have "benefitted from Cyber & Digital Training" in partnership with the DCCP since 2018. Washington has also provided CSIRT Development Mentoring Frameworks to "donate knowledge" to local governments, including coordinating and providing cybersecurity awareness campaigns, assessing organizational cybersecurity policies, and facilitating the implementation of cybersecurity training programs in the academic sector (US Embassy in Ghana, 2023; Ramim & Hueca, 2021). At the regional level, US and the AU Commission have collaborated on CCB workshops to create cyber strategies, legislations, and the development national CERT/CSIRTs (Amazouz, 2020).

The governance level: Conditionality and competing norms

Finally, the EU, the US and China have sought to export their preferred norms and governance models, project soft power influence, and ultimately build further connections with recipients in their provisions of capacity building assistance. Foremost, the importance of EU digital development programs for promoting EU values and interests has been

explicitly stated in EU policy documents, including operational guidance and SWDs concerning the AU-EU Digital4Development hub (European Commission, 2022; European Union 2021, p. 2). As the emblematic "normative power" actor (Manners, 2002), Brussels has levied its digital development investments to shape the national regulations of third countries and export the "Made in Europe" solutions to partner countries, including through capacity building initiatives (European Commission, 2017, p. 15). For example, Kenya has been regarded by EU policymakers as the successful case for EU capacity building efforts, after it implemented "GDPR-like" data privacy legislation into its national cybersecurity framework (Interviewee 2). Moreover, the EU has recently invested in an "e-ID GDPR alignment" initiative for Nigeria, which seeks to bolster Nigeria's privacy and data protection laws, especially in the wake of Nigeria's turn towards a more a Chinese-oriented approach to internet governance (Denis, 2021). As Africa's largest trading partner, the EU has also provided capacity building for digital development at the governance level (e.g. on e-governance and data protection) to encourage harmonization between the EU and African markets (Fritzsche & Spoiala, 2022).

To this end, *conditionality* instruments in EU digital development financing have been considered by the EU as a way to encourage the development of external rules in line with EU values and strategic interests (Interviewee 5; Renard, 2018). Accordingly, EU external capacity building assistance has often remained conditional upon a third country's (eventual) signing of the Budapest Convention, the EU's preferred framework for responsible behaviour in cyberspace (Interviewee 3). Partner countries must also be receptive to the EU's normative goal of an open, free, and secure internet (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020).

Separately, the US has also sought to shape global standards and national cybersecurity legislation through initiatives led by USAID (Calzati, 2022), including the DTA and the DCCP. Recently, the importance of digital development initiatives was reaffirmed by Secretary of State Blinken's declaration that, "We want to shape the standards that govern new technology[...] We [want] to make sure that the United States remains the world's innovation leader and standard setter" (United States Department of State, 2021).Thus, the government has emphasized its "proactive" and "expanded" participation in developing norms, standards, and principles which impact cyberspace as a key area of action for "strengthen[ening] and build[ing]" partners' capacity building for digital development, and "aligning [their] rights-respecting approaches to digital and data governance" with the US (US State Department, 2024).

Meanwhile, China has also used capacity building and its involvement in technical standard setting to promote its approach to digital development governance, although to a lesser extent than the US and the EU. In multilateral, diplomatic contexts, Beijing has frequently signaled its intention to increase its capacity building efforts, particularly in the domain of human capacity building and norms, including promoting a "community of shared future" in cyberspace (Minlu, 2022; Xinhua, 2021). In this regard, China has sought to encourage collaboration in internet governance, security, and development multilaterally through the Forum of China-Africa Cooperation (FOCAC).

In 2021, Beijing has announced a *China-Africa Partnership Plan on Digital Innovation* to build "cooperation platforms to promote digital progress through exchanges" in the form of high-level dialogues (Ministry of Foreign Affairs of the People's Republic of China, 2021). Additionally, China has offered training to government officials of BRI member countries on cyber-related governance topics, such as "Cyberspace Management"

and cybersecurity, including to Egypt, Libya, Tanzania and Uganda (Shabhaz, 2018). These activities have served as pathways to promote Beijing's approach to global standard-setting, including internet governance and shaping technical standards in the area of 5G (Rühlig, 2022).

Conclusion: Perceptions of geostrategic competition and calibrating capacity building assistance for digital development in Africa

This article examined the relationship between capacity building tools and donors' perceptions of strategic advantage through the perspective of *networked competition*. Focusing upon EU, US, and Chinese perceptions of such assistance and their deployment of capacity building tools in partnership with multiple African states has enabled me to probe the plausibility of my framework in these contexts.

Specifically, my empirical analysis revealed a rising competitive, geostrategic undercurrent in EU, US, and Chinese official discourses about capacity building assistance for digital development. At the level of digital infrastructural assistance, I examined how China has achieved a first-mover advantage in building Africa's digital infrastructural capacity, eschewing conditionality measures. While the EU and US have been slower to invest in infrastructure, they have advanced their own major infrastructural initiatives (viz. the Global Gateway and the DTA) as explicitly competitive alternatives to China's BRI projects and connectivity initiatives. As evidenced by the case of SeaMeWe-6 undersea cable competition, the US leveraged has also leveraged softer capacity building tools—such as skills building—as a carrot for potential partners to choose their preferred alternative over Chinese investors.

Examining EU and US donations of capacity building assistance at the sectoral level suggests that they have been characterized by Washington and Brussels' (competing) efforts

to offset the influence of Chinese digital infrastructural assistance on recipients, including using conditionality measures. This is evidenced in the cases of EU action in Tanzania and US efforts in Tanzania, Ghana, and Burkina Faso. By contrast, evidence of Chinese-funded sectoral capacity building in Tanzania and Ghana indicates limited transfers of substantive cybersecurity and digital skills, which may suggest a strategy of restriction deployed by the PRC.

At the governance level, the EU, US, and China have all encouraged recipients to adopt their preferred standards in cybersecurity, technology, and data protection through capacity building assistance channels in various African countries, including Tanzania, Nigeria, and Kenya. By calibrating their instruments to outcompete each other—sometimes in explicit terms, as in the case of Tanzania and Ghana—it appears that all three donors have engaged in targeted empowerment practices to hedge against each other's influence.

Below, I discuss which factors may have shaped variation in donors' provision of certain capacity building assistance tools. Next, I elaborate the broader research agenda introduced by this article, including future areas for research, and discuss preliminary conclusions.

Supply-side factors mediating the provision of capacity building assistance in the context of networked competition

Considering which factors may have shaped variation in donors' provision of assistance, I theorized that the donor's domestic capacity, normative approach to development, and supply-side incentives for competition (e.g. outcompeting rivals) were causally relevant factors. On these bases, I expected that Brussels and Washington would engage with conditionality instruments, Beijing to favor restrictive knowledge transfers, and

all three donors engaging in targeted empowerment practices, shaped by their strategic goals and interests.

My empirical analysis illuminated how these factors could mediate donors' varying strategies of assistance. First, empirical evidence of sectoral-level capacity building tools provided by the EU, US, and China supports the significance of normative/cultural characteristics as mediating factors. For one, these variables reflect scholarly consensus that the US and the EU have a strong tradition of providing "human-oriented" capacity building initiatives in their development cooperation (Collett & Barmpaliou, 2021). However, China's distinctive approach to knowledge transfers can also be situated within the context of the PRC's longstanding ideological approach to development. Chinese domestic discourses in political leadership and academic circles have consistently characterized Chinese development cooperation as eschewing the standardized Western model exported by developed actors such as the EU and the US (Schwarz & Rudyak, p. 41). Rather, China's approach to development, according to domestic academics and political leaders, is constructed to "fills in the gaps" of Western aid by solving "practical problems" (e.g. providing material assistance) and sharing "proven development experience" and knowledge based on China's own development experience (translations in Schwarz & Rudyak, p. 40-42). As explored by this article, country case studies of Ghana (Wang & Elliot, 2014 p. 1026; Kernen & Lam, 2014) and Tanzania (USAID, 2023; Makundi et al., 2016) partly support this assertion, as they have documented how Chinese companies have provided (restrictive) *company-specific* knowledge and skills as opposed to general sectoral knowledge and problem-solving.

Yet, the relationship between Chinese state-owned enterprises (SOEs) and the PRC's development finance structure may also incentivize the restriction of substantive knowledge

transfers. As part of China's overseas investment approach, internationally competitive Chinese SOEs, such as ZTE and Huawei, are offered "strategic lines of credit", which entail a financing platform with export sellers' and buyers' credits, import credits, and preferential foreign loans to secure overseas business (Brautigam, 2011). This global development strategy ties into Beijing's approach to domestic production. Unlike the US and EU cases, China views its domestic production inputs as "strategically important commodities" and therefore overproduces these materials beyond domestic demand (Dreher et al., 2021, p. 143). These materials feed into Beijing's overseas grant and loan-financed projects, which generally "involve physical construction; require construction inputs oversupplied in China; and they often obligate recipients to import these inputs on a preferential basis" (Dreher et al., 2021, p. 143-44). Accordingly, the incentives for maintaining overseas demand and dependence on Chinese technologies and technical expertise may be strategically and financially intertwined (cf. Kernen & Lam, 2014; Hall & Krolikowski, 2022). However, further evidence is required to make causal conclusions as to whether donors' relationship with intermediary firms explains their engagement with conditionality or restriction, particularly as there appears to be normative and cultural dimensions which also shape donors' provision of assistance.

Relatedly, providing capacity building assistance at the governance level—or at least stating this ambition publicly—can enable donors to narratively position themselves as global digital leaders. The EU's Global Gateway initiative, for instance, has been marketed as both a response to China's BRI (Haroche, 2022) and as a way of signaling to EU Member States the Commission's ambition to ensure European resilience and to speak in geopolitical terms (Haroche, 2022; Carver, 2024). Similarly, Washington's strategy is both self-referential (seeking to "ensure U.S. foreign policy delivers on the issues that matter most to the lives and livelihoods of the American people") and it publicly contrasts the US approach

to digital partnerships EU and China (US Department of State, 2024). As previously described, China has also directly defined its approach to digital development in opposition to Western competitors; scholars have argued that the PRC's media coverage of Chinese SOEs' efforts to build the capacity of local sectors in Africa, as evidenced by China Daily and others, "serves as both encouragement [to companies] and propaganda" (Kernen & Lam, 2014, p. 1072).

Overall, my empirical findings support the plausibility that EU, US, and Chinese capacity building practices have been shaped by their distinct domestic characteristics (including institutional and juridical contexts), normative orientations, and relationships to African states, as well as varying degrees of control over the intermediary providers of capacity building assistance.

Capacity building as strategic alignment and geostrategic competition

By foregrounding the strategic dimension to capacity building assistance in the context of EU, US, and Chinese competition over digital development in Africa, this article has unveiled several areas for further research.

First, this article focused upon *donors' perceptions* about the strategic import of capacity building assistance for digital development and their engagement with such instruments in specific countries in Africa. Accordingly, there is greater scope for probing the article's theoretical expectations in other country contexts, especially the recipient side of digital development. While donor-recipient interactions "continue to be heavily structured fields of power with significant power imbalances between donors and recipients" (Baran, 2022, p. 754), recipients have agency and strategic interests of their own (Allen & Lime, 2024; Edmunds & Juncos, 2019). Developments such as the inclusion of two more African countries into BRICs (Ismail, 2023), the emergence of "Smart Alliance Africa" and calls for

a “Digital Non-Aligned Movement” (Reddy, 2021), and the re-election of US President Donald Trump (Emoruwa, 2024) could signal a changing dynamic in donors’ provision of assistance to African states and an increase in recipients’ bargaining power (see also Wang & Elliot, 2013, p. 1024). In this regard, emerging literature on African states’ strategic interests in cyber partnerships (Allen & La Lime, 2024, p. 11) suggests that geopolitical perceptions and strategic interests can underlie capacity building cooperation for *both* donors and recipients. Future studies could explore the recipient side of digital development cooperation in greater depth, including which factors shape recipient states’ acceptance of certain types of digital development assistance, on-the-ground implementation of such practices, their decision(s) to remain aligned (or not) with the donor over time.

To be sure, the implementation of planned capacity building outcomes is shaped by local interests and a variety of different actors which implicate effectiveness (Edmunds & Juncos, 2019; Allen & La Lime, 2024). Accordingly, the effectiveness of capacity building assistance for digital development (and effectiveness for *who*) constitutes another important area for future research. At the time of writing, data availability and temporal limitations constrain such observations, as several major EU and US digital development projects, such as the Global Gateway and the DTA, remain at nascent stages. Similarly, the BRI is arguably still in its “infancy” for analyses (Hall & Krolikowski, 2022, p. 15).

Beyond the context of capacity building tools for digital development, extant research on the effectiveness of competing development assistance projects suggests a complex picture. Scholarship has emphasized the importance of contextual factors, including past colonial relationships between the donor and the recipient (Carver, 2024), mutual trust, and diplomatic and economic relationships in other policy issue areas which generally affect donor-recipient interactions (Hall & Krolikowski, 2022). For instance,

scholars and EU officials have acknowledged that conditionality measures do not guarantee cooperation (Interviewee 5; Blauberger & Van Hüllen, 2021). Indeed, while some scholars have argued that China is "innately appealing" for African recipients (Tugendhat & Voo, 2021, p. 4), recent analysis has highlighted a more complex trend: whereas Chinese aid improved perceptions of the US, the UK, and France, in African publics, US aid improved perceptions of the US in recipient countries (Blair et al., 2022).

Notwithstanding these debates, examining donors' perceptions of capacity building assistance as constituting strategic tool(s) is critical for making sense of the nexus between cyber and digital capacity, geopolitical competition, and weaponized interdependence concerns in our digital age. As techno-geopolitical competition between the US, the EU, and China remains an overarching strategic issue, the import of capacity building assistance for these powerful donors is unlikely to diminish. (Recall that the 2016 Trump administration introduced the Prosper Africa and DCCP initiatives, and they remain active US investments in the region.)

Overall, digital development assistance patterns across the African continent reveal how so-called "peripheral" areas of the global digital network play a significant role in the dynamics of strategic competition between three global powers: the EU, US, and China. Examining one facet of this wider phenomenon, this article has chiefly argued that Washington, Brussels, and Beijing have perceived capacity building assistance for digital development as creating opportunities to position themselves favorably in the global digital environment and to hedge against geopolitical rivals. Here, it is worth reflecting upon Nnenna Ifeanyi-Ajufo's warning that "transfers of capacity and expertise must be strategized to ensure that digital cooperation does not translate into [Africa's] digital dependence," (2023, p. 154). Given these policy imperatives and recent developments in the literature on

weaponized interdependence, interrogating the strategic dimension to capacity building assistance for digital development is a promising area for future research.

Chapter 4 References

African Union. (2020). The Digital Transformation Strategy for Africa (2020-2030).

AU-EU Digital Economy Task Force. (2019). New Africa-Europe Digital Economy Partnership. https://international-partnerships.ec.europa.eu/system/files/2021-01/new-africa-eu-digital-economy_en_0.pdf.

Agbebi, M. (2018). China in Africa's Telecom Sector: Opportunities for Human Capital Development? A Case of Huawei in Nigeria. *Human Resource Development International* 21(5), 532–51. https://doi.org/10.1080/13678868.2018.1512232.

———. (2022, February 1). China's Digital Silk Road and Africa's Technological Future. *Carnegie Endowment*. https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-.

Agbebi, M., Xue, G., & Yu, Z. (2021). China-Powered ICT Infrastructure: Lessons from Tanzania and Cambodia. *South African Institute of International Affairs*. https://saiia.org.za/research/china-powered-ict-infrastructure-lessons-from-tanzania-and-cambodia/.

Aiken, K., & Kumar, S. (2019, October 14). Unpacking the GGE's framework on responsible state behaviour: Capacity Building. *Global Partners Digital.* https://www.gp-digital.org/publication/unpacking-the-gges-framework-on-responsible-state-behaviour-capacity-building/.

Allen, N.D.F. & La Lime, M. (2024). Cyberspace and the international politics of African agency. *Journal of Strategic Studies,* 1-26. https://doi.org/10.1080/01402390.2024.2330074.

Alper, A. & Psaledakis, D. (2021, December 16). UPDATE 10-U.S. curbs Chinese drone maker DJI, other firms it accuses of aiding rights abuses. *Reuters.* https://www.reuters.com/article/usa-china-actions-idCNL1N2T11DU.

Amazouz, S. (2020). Cyber Capacity-Building and International Security. In E. Tikk & M. Kerttunen (Eds.), *Routledge Handbook of International Cybersecurity* (pp. 201-213). Routledge.

Baran, K. (2022). Rethinking recipient agency: what can we learn from Haitian accounts? *Third World Quarterly* (43), 742-759. https://www.tandfonline.com/doi/full/10.1080/01436597.2021.2017276.

Bermeo, S.B. (2018). *Targeted Development: Industrialized Country Strategy in a Globalizing World.* Oxford University Press.

Bialasiewicz, L. (2015). *Europe in the World: EU Geopolitics and the Making of European Space.* Routledge.

Blauberger, M., & V. Van Hüllen. (2021). Conditionality of EU Funds: An Instrument to Enforce EU Fundamental Values? *Journal of European Integration* 43 (1), 1–16. https://doi.org/10.1080/07036337.2019.1708337.

Blair, R.A., Marty, R., & Roessler, P. (2022). Foreign Aid and Soft Power: Great Power Competition in Africa in the Early Twenty-first Century. *British Journal of Political Science* 52(3), 1355-1376. https://doi.org/10.1017/S0007123421000193.

Brautigam, D. (2011). Chinese Development Aid in Africa: What, Where, Why, and How Much? *SSRN.* http://dx.doi.org/10.2139/ssrn.2013609.

Borrell, Josep. (2024, September 26). Op-Ed by the High Representative/Vice-President Josep Borrell: the Draghi report and Europe's geopolitical future. *European Union External Action Service.* https://www.eeas.europa.eu/eeas/op-ed-high-representativevice-president-josep-borrell-draghi-report-and-europes-geopolitical-future_en.

Brock, J. (2023a, March 24). U.S. and China wage war beneath the waves – over internet cables. *Reuters.* https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

———. (2023b, April 6.) China plans $500 million subsea internet cable to rival US-backed project. *Reuters.* https://www.reuters.com/world/china/china-plans-500-mln-subsea-internet-cable-rival-us-backed-project-2023-04-06/.

Calzati, S. (2022). 'Data Sovereignty' or 'Data Colonialism'? Exploring the Chinese Involvement in Africa's ICTs: A Document Review on Kenya. *Journal of Contemporary African Studies 40* (2), 270-285. https://doi.org/10.1080/02589001.2022.2027351.

Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy 31* (8), 1-37. https://doi.org/10.1080/13501763.2023.2295523.

Cha,V.D. (2023). Collective Resilience: Deterring China's Weaponization of Economic Interdependence. *International Security 48*(1), 91–124. https://doi.org/10.1162/isec_a_00465.

Christou, G. (2016). *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy.* Hampshire: Palgrave MacMillan.

Collett, R. (2021). Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures. *Journal of Cyber Policy 6*(3), 298–317. https://doi.org/10.1080/23738871.2021.1948582.

Collett, R., & Barmpaliou, N. (2021). International Cyber Capacity Building: Global Trends and Scenarios. *European Institute for Security Studies*. https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.

Council of the European Union Presidency (2016). *Cyber capacity building: towards a strategic European approach* [8732/1/16].

Denis, B. (2021). The Rise of Africa's Digital Economy: The European Investment Bank's Activities to Support Africa's Transition to a Digital Economy. *European Investment Bank*. https://doi.org/10.2867/135126.

Dizolele, M.P. (Host). (2024, May 2). *The Twists and Turns of U.S.- Tanzania Bilateral Relations (Ambassador Michael Battle)*. CSIS. https://www.csis.org/analysis/twists-and-turns-us-tanzania-bilateral-relations.

Dreher, A., Fuchs, A., Parks, B., Strange, A., & Tierney, M.J. (2021). Aid, China, and Growth: Evidence from a New Global Development Finance Dataset. *American Economic Journal: Economic Policy 13* (2), 135–74. DOI: 10.1257/pol.20180631.

Drezner, D.W., Farrell, H., & Newman, A.L. (2021). *The Uses and Abuses of Weaponized Interdependence*. Brookings Institution Press.

The Economist. (2022, February 19). How Chinese Firms Have Dominated African Infrastructure. https://www.economist.com/middle-east-and-africa/how-chinese-firms-have-dominated-african-infrastructure/21807721.

Edmunds, T. & Juncos, A.E. (2019). Constructing the capable state: Contested discourses and practices in EU capacity building. *Cooperation and Conflict 55*(1), 3-21. https://doi.org/10.1177/0010836719860885.

Ehl, D. (2022, February 8). Africa Embraces Huawei Technology despite Security Concerns. *Deutsche Welle*. https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700.

Erforth, B. & Fritzsche, K. (2022). Towards a Digital Development Partnership That Meets African Interests. *Heinrich Böll Stiftung Institute*. https://us.boell.org/sites/default/files/2022-01/20220127-HB-paper 01-digital development-01.pdf.

Emoruwa, A. (2024, November 8). What Trump's win means for Africa's trade and investment. *Open Democracy.* https://www.opendemocracy.net/en/trump-win-africa-diplomacy-america-first-trade-investment/.

European Commission. (2017). *Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy* [Working paper, SWD(2017) 157 final].

———. (2021a, December 1). *Global Gateway: Up to €300 Billion for the European Union's Strategy to Boost Sustainable Links around the World* [press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6433.

———. (2021b). 2030 Digital Compass: the European way for the Digital Decade [COM/2021/118 final].

———. (2022a). *EU-Africa: Global Gateway Investment Package*. https://ec.europa.eu/commission/presscorner/detail/en/fs_22_1117.

———. (2022b). *African-European Digital Innovation Bridge Network*.

https://cordis.europa.eu/project/id/101017105.

———. (2023). *Global Gateway: EU launches Digital Economy Package for Kenya to boost connectivity, skills and inclusive governance.*

———. (n.d.-a) *AU-EU Digital for Development (D4D) Hub: Shaping a joint digital future.* https://international-partnerships.ec.europa.eu/policies/programming/projects/au-eu-digital-development-d4d-hub-shaping-joint-digital-future_en.

———. (n.d.-b). *Digital.* International Partnerships. https://international-partnerships.ec.europa.eu/policies/global-gateway/digital_en.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2020). *The EU's Cybersecurity Strategy for the Digital Decade* [JOIN/2020/18final].

European Union. (2021). *ANNEX 3: Action Document for Digital4Tanzania – e-Governance Support Program*. Retrieved from https://www.gtai.de/resource/blob/788132/e262205f40141c2ea2c13c84f61c4b27/PRO20220127788124%20-%20Annex3.PDF.

———. (2022). *THE EU-NIGERIA DIGITAL ECONOMY PACKAGE (2021-2024).* https://ec.europa.eu/commission/presscorner/api/files/attachment/871307/GG_Nigeria%20factsheet.pdf.

———. (2023, October). EU-Africa: Global Gateway Investment Package - Digital transition. https://international-partnerships.ec.europa.eu/document/download/ab8ab1c6-cf1e-46a8-a871-cb529a7d146a_en?filename=GG_Factsheet_Africa_Digital%20Transition.pdf.

Farrell, H., & Newman, A.L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security* 44 (1), 42–79. https://doi.org/10.1162/isec_a_00351.

Feldstein, S. (2020). Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa. https://www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf.

Fritzche, K & Spoiala, D. (2022). The EU–AU Digital Partnership. In C. Daniels, B. Erforth, & C. Teevan (Eds.), *Africa–Europe Cooperation and Digital Transformation* (pp. 17-31). Routledge.

Ford, C. A. (2020, November 2020). The Evolution of International Security Capacity Building: Remarks - United States Department of State. *U.S. Department of State*. https://2017-2021.state.gov/the-evolution-of-international-security-capacity-building/index.html.

General Secretariat of the Council. (2018). *EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)* [10496/18]. Council of the European Union.

———.(2022). Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade. [7290/21]. Council of the European Union.

Gjesvik, L. (2023). "Private Infrastructure in Weaponized Interdependence." *Review of International Political Economy* 30(2), 722-746. https://www.tandfonline.com/doi/full/10.1080/09692290.2022.2069145.

Gravett, W.H. (2022). Digital Neocolonialism: The Chinese Surveillance State in Africa. *African Journal of International and Comparative Law 30*(1), 39–58. http://dx.doi.org/10.3366/ajicl.2022.0393.

Hafner-Burton, E.M., Kahler, M., & Montgomery, A.H. (2009). Network Analysis for International Relations. *International Organization* 63(3), 559-592. https://doi.org/10.1017/S0020818309090195.

Hall, T., & Krolikowski, A. (2022). Making Sense of China's Belt and Road Initiative: A Review Essay. *International Studies Review 24*(3), 1-18. https://doi.org/10.1093/isr/viac023.

Hathaway, M., & Spidalieri, F. (2021). Integrating Cyber Capacity into the Digital Development Agenda. *Global Forum on Cyber Expertise Foundation*. https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf.

Haroche, P. (2022). A 'geopolitical commission': Supranationalism meets global power competition. *JCMS: Journal of Common Market Studies 61*(4), 970–987. https://doi.org/10.1111/jcms.13440.

Hernandez, J.C. (2021, October, 11). China's National Security Law for Hong Kong, Explained. *The New York Times*. https://www.nytimes.com/2020/06/30/world/asia/hong-kong-security-law-explain.html.

Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society 33*(2), 224–42. https://doi.org/10.1080/13600826.2019.1569502.

Huang, Y. (2020). An interdependence theory of wedge strategies. *Chinese Journal of International Politics 13*(2), 253–86. https://doi.org/10.1093/cjip/poaa004.

Hurel, L. M. (2022). Interrogating the Cybersecurity Development Agenda: A Critical Reflection. *The International Spectator 57*(3), 66–84. https://doi.org/10.1080/03932729.2022.2095824.

Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. *Policy Design and Practice* 6 (2), 146-159. https://doi.org/10.1080/25741292.2023.2199960.

Ismail, S. (2023, August 24). 'A wall of BRICS': The significance of adding six new members to the bloc. *Aljazeera.* https://www.aljazeera.com/news/2023/8/24/analysis-

wall-of-brics-the-significance-of-adding-six-new-members.

Kadiri, G., & Tilouine, J. (2018, January. 26). A Addis-Abeba, Le Siège de l'Union Africaine Espionné Par Pékin. *Le Monde*. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a Security Threat. NATO CCDCOE. https://ccdcoe.org/library/publications/huawei-5g-and-china-as-a-security-threat/.

Kernen, A. & Lam, K.N. (2014). Workforce Localization among Chinese State-Owned Enterprises (SOEs) in Ghana. *Journal of Contemporary China* (23)90, 1053-1072. https://doi.org/10.1080/10670564.2014.898894.

Kokas, A. (2022). *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty.* Oxford University Press.

Kuner, C. (2019). The Internet and the Global Reach of EU Law. In Cremona, M. & Scott, J., (Eds.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law* (pp. 112-145). Oxford University Press.

Lopez, T.C. (2023, September 12). DOD's Cyber Strategy Emphasizes Building Partner Capacity. *U.S. Department of Defense*. https://www.defense.gov/News/News-Stories/Article/Article/3523840/dods-cyber-strategy-emphasizes-building-partner-capacity/.

Loughlan, V., Olsson, C., & Schouten, P. (2014). Mapping 1. In C. Aradau, J. Huysmans, A. Neal, & N. Voelkne (Eds.), *Critical Security Methods: New Frameworks for Analysis* (pp. 23-54). Routledge.

Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict, *Journal of Strategic Studies 46*(3), 570-594. https://doi.org/10.1080/01402390.2022.2104253.

Makundi, H., Huyse, H., & Develtere, P. (2016). Cooperation between China and Tanzania on ICT: Fish, Fishing Tackle or Fishing Skills? *Journal of Chinese Economic and Business Studies* 14 (2), 129–49. https://doi.org/10.1080/14765284.2016.1174459.

Manners, Ian. (2002). Normative Power Europe: A Contradiction in Terms? *Journal of Common Market Studies 40*(2), 235-58. https://doi.org/10.1111/1468-5965.00353.

Meijer, H., & Simón, Luis. (2021). Covert balancing: Great Powers, secondary states and US balancing strategies against China. *International Affairs* 97 (2), 463–481. https://doi.org/10.1093/ia/iiaa228.

Ministry of Foreign Affairs of the People's Republic of China. (2015, September 27). Xi Jinping Delivers Speech at High-level Roundtable on South-South Cooperation, Expounding on Cooperation Initiatives on South-South Cooperation in the New Era and Stressing to Uplift South-South Cooperation Cause to a New High.

https://www.mfa.gov.cn/eng/zy/jj/2015zt/xjpdmgjxgsfwbcxlhgcl70znxlfh/202406/t20240606_11381569.html.

———. (2016, September 7). Position Paper of the People's Republic of China At the 71st Session of the United Nations General Assembly. https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367342.html.

———. (2021, August 24). China will work with Africa to formulate and implement a China-Africa Partnership Plan on Digital Innovation. https://www.fmprc.gov.cn/eng/wjbxw/202108/t20210825_9134687.html.

———. (2024, April 19). *The Hypocrisy and Facts of the United States Foreign Aid.* https://www.mfa.gov.cn/mfa_eng/xw/wjbxw/202405/t20240530_11344003.html.

———. (2024, September 24). Bearing in Mind Our Common Future and Jointly Building a Better Tomorrow. https://www.mfa.gov.cn/eng/xw/zyjh/202409/t20240924_11495643.html.

Minlu, Z. (2022, August 9). China Calls on UN to Support Capacity-Building in Africa. *China Daily*. http://global.chinadaily.com.cn/a/202208/09/WS62f1b116a310fd2b29e710b7.html.

Munga, J. & Monye, E. (2024). Tracking Progress of the U.S. Digital Transformation With Africa Initiative. *Carnegie Endowment.* https://carnegieendowment.org/posts/2024/03/tracking-progress-of-the-us-digital-transformation-with-africa-initiative?lang=en.

Narlikar, A. (2021). Must the Weak Suffer What They Must? The Global South in a World of Weaponized Interdependence. In D.W. Drezner, H. Farrell, & A.L. Newman (Eds.), *The Uses and Abuses of Weaponized Interdependence* (pp. 289-304). Brookings Institution Press.

Oppenheimer, Harry. (2023). Developing Digital Capacity: How Foreign Assistance Shapes Institutions. *SSRN Scholarly Paper* (unpublished manuscript). https://doi.org/10.2139/ssrn.441733.

Park, Y.J., & Tang, X. (2021). Chinese FDI and Impacts on Technology Transfer, Linkages, and Learning in Africa: Evidence from the Field. *Journal of Chinese Economic and Business Studies* 19(4), 257–68. https://doi.org/10.1080/14765284.2021.1996191.

Pawlak, P. (2014). In G. Giacomello (Ed*.), Security in Cyberspace: Targeting Nations, Infrastructures, Individuals* (pp. 39-58). Bloomsbury Publishing.

Pawlak, P. (2016). Capacity Building in Cyberspace as an Instrument of Foreign Policy. *Global Policy. 7*(1), 83-92. https://doi.org/10.1111/1758-5899.12298.

———. (2018). *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building* (Report: ISBN 978-92-9198-756-6). EUISS Task Force for Cyber Capacity Building, European Commission. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pd

f.

Pawlak, P., & Barmpaliou, P-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy 2* (1): 123-144. https://doi.org/10.1080/23738871.2017.1294610.

———. (2023). *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building: Second Edition.* Tallinn: European Union. https://www.eucybernet.eu/wp-content/uploads/2023/11/operational-guidance-for-the-eu-international-cooperation-on-ccb-1-1.pdf.

Peace Cable International Network Co., Ltd. (2018). PEACE Cable System. http://www.peacecable.net/.

———. (n.d.) PEACE Completed Construction from Pakistan to France – Peace. Last accessed 3 November 2023. http://www.peacecable.net/news/Detail/16641.

Pence, M. (2018, October 4). Remarks by Vice President Pence on the Administration's Policy Toward China. *The White House*. https://trumpwhitehouse.archives.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china/.

Perry, S., & Menski, M. (2021, June 29). US Finance Agencies in Africa. *White & Case LLP*. https://www.whitecase.com/insight-alert/us-finance-agencies-africa.

Pohle, J. & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, 14, 13–27. https://doi.org/10.1002/poi3.296.

Portela, C. (2007). Aid Suspensions as Coercive Tools? The European Union's Experience in the African-Caribbean-Pacific (ACP) Context. *Review of European and Russian Affairs* 2(3): 38–53. https://doi.org/10.22215/rera.v3i2.155.

Prontera, A., & Quitzow, R. (2023) Catalytic Power Europe: Blended Finance in European External Action. *Journal of Common Market Studies 61*(4), 988-1006. https://doi.org/10.1111/jcms.13442.

Prosper Africa. (2021, June 1). 'Doing Business in Africa and Leveraging the Influence of the African Diaspora – an Interview with Thierry Wandji.' USDTA. https://www.prosperafrica.gov/blog/doing-business-in-africa-and-leveraging-the-influence-of-the-african-diaspora/.

Ramim, M. & Hueca, A. (2021). Cybersecurity Capacity Building of Human Capital: Nations Supporting Nations. *Online Journal of Applied Knowledge Management* 9 (1). https://doi.org/10.36965/OJAKM.2021.9(2)65-85.

Reddy, L. (2021). Is There Space for a Digital Non-Aligned Movement? *Hague Centre for Strategic Studies*. https://hcss.nl/report/is-there-space-for-a-digital-non-aligned-movement/.

Ren, X. (2019, April 27). Digital Silk Road Helping Developing Countries. *China Daily*. https://www.chinadaily.com.cn/a/201904/27/WS5cc3a6e7a3104842260b8add.html.

Renard, T. (2018). EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society 19(*3), 321–37. https://doi.org/10.1080/23745118.2018.1430720.

Rühlig, T. (2022). Chinese Influence through Technical Standardization Power. *Journal of Contemporary China* 32(139), 54-72. https://doi.org/10.1080/10670564.2022.2052439.

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy 45* (1), 7-44. https://doi.org/10.1080/13523260.2023.2296739.

Schwarz, R. & Rudyak, M. (2023). China's development co-operation. *OECD Development Cooperation Working Papers.* https://doi.org/10.1787/22220518.

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive Design: Concepts and Processes.* Routledge, Taylor & Francis.

Secretary Antony J. Blinken on the Modernization of American Diplomacy. (2021, October 27). *United States Department of State*. https://www.state.gov/secretary-antony-j-blinken-on-the-modernization-of-american-diplomacy/.

Seidl, T. (2024). Charting the Contours of the Geo-Tech World. *Geopoltics 29*(5), 2033-2045. https://doi.org/10.1080/14650045.2024.2333358.

Shabhaz, A. (2018). The Rise of Digital Authoritarianism. *Freedom House*. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

Tecott Metz, R. (2023). The Cult of the Persuasive: Why U.S. Security Assistance Fails." *International Security* 47 (3), 95–135. https://doi.org/10.1162/isec_a_00453.

Tiirmaa-Klaar, H. (2016). Building national cyber resilience and protecting critical information infrastructure. *Journal of Cyber Policy 1*(1), 94-106. https://doi.org/10.1080/23738871.2016.1165716.

Tugendhat, H. (2021). Connection Issues: A Study on the Limitations of Knowledge Transfer in Huawei's African Training Centres. *Journal of Chinese Economic and Business Studies 1*9 (4), 359–85. ttps://doi.org/10.1080/14765284.2021.1943194.

———. (2020). How Huawei Succeeds in Africa: Training and Knowledge Transfers in Kenya and Nigeria. *China Africa Research Initiative* (Johns Hopkins University). http://www.sais-cari.org/publications.

Tugendhat, H. & Voo, J. (2021). China's Digital Silk Road in Africa and the Future of Internet Governance. *China Africa Research Initiative* (Johns Hopkins University). https://www.econstor.eu/bitstream/10419/248239/1/sais-cari-pb60.pdf.

UNCTAD. (2019). Donor Support to the Digital Economy in Developing Countries: A 2018 Survey of Public and Private Organizations. https://unctad.org/system/files/official-document/tn_unctad_ict4d13_en.pdf.

UNIDIR. (2024, May 16). Inaugural Global Roundtable on ICT Security Capacity Building: Recap and Key Highlights. https://unidir.org/inaugural-global-roundtable-on-ict-security-capacity-building-recap-and-key-highlights/.

USAID. (2020). *Digital Download: A Year in Review*. https://www.usaid.gov/sites/default/files/documents/Digi_Dwnld_V8_web.pdf.

———. (2022, September 1). *Digital Connectivity and Cybersecurity Partnership* (DCCP). https://www.usaid.gov/digital-development/digital-connectivity-cybersecurity-partnership.

———.(2023, March 23). USAID's Policy Framework. https://www.usaid.gov/policy/documents/mar-23-2023-usaids-policy-framework.

———. (n.d.). Digital Ecosystem Country Assessments. https://www.usaid.gov/digital-strategy/implementation-tracks/track1-adopt-ecosystem/digital-ecosystem-country-assessments.

US Department of State. (2024). *United States International Cyberspace & Digital Policy Strategy.* https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

———. (n.d). Digital Transformation with Africa. https://www.state.gov/digital-transformation-with-africa/.

US Embassy in Ghana. (2023). Ambassador Palmer's Remarks at Tech In Ghana. https://gh.usembassy.gov/amb-palmers-remarks-at-tech-in-ghana/.

US Embassy Gaborone. (2023). USTDA Supports Nationwide Digital Infrastructure Expansion in Botswana. https://bw.usembassy.gov/ustda-supports-nationwide-digital-infrastructure-expansion-in-botswana/.

Wang, F-L., & Elliot, E.A. (2014). China in Africa: presence, perceptions and prospects. *Journal of Contemporary China* 23 (90), 1012-1032. https://doi.org/10.1080/10670564.2014.898888.

The White House. (2021, June 12). FACT SHEET: President Biden and G7 Leaders Launch Build Back Better World (B3W) Partnership. https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/12/fact-sheet-president-biden-and-g7-leaders-launch-build-back-better-world-b3w-partnership/.

———. (2023, March 30). FACT SHEET: Vice President Harris Announces Initiatives to Deepen the U.S. Partnership with Tanzania. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/30/fact-sheet-vice-president-harris-announces-initiatives-to-deepen-the-u-s-partnership-with-tanzania-2/.

Xinhua. (2021, April 28). Chinese Luban Workshop Launched in Ethiopia to Boost Vocational Training. http://www.xinhuanet.com/english/2021-04/28/c_139913065.htm.

———. (2022, June 16). China's Digital Silk Road solution to corruption in Africa: AU experts. *Belt and Road Portal.* https://eng.yidaiyilu.gov.cn/p/253055.html.

Zajácz, R. (2019). *Reluctant Power: Networks, Corporations, and the Struggle for Global Governance in the Early 20th Century* (MIT Press).

Zhao, M. (2019). Is a New Cold War Inevitable? Chinese Perspectives on US–China Strategic Competition. *The Chinese Journal of International Politics 12 (*3), 371-394. https://doi.org/10.1093/cjip/poz010.

Appendix A: Common dimensions of capacity building assistance for digital development

Three common dimensions of capacity building assistance for digital development cooperation			
Level of intervention	**Example digital development cooperation area**	**Examples of capacity building assistance tools**	
		'Cyber' capacity building*	**'Digital' capacity building***
		*Precise distinctions between cyber and digital capacity building definitions vary across different communities of practice.	
Infrastructural (internet "backbone")	Critical infrastructure assistance and connectivity	Digital and cyber resilience initiatives, including integrating cybersecurity technologies into CNI (e.g. "securing by design")	Maintenance of digital technologies: digitalization of services, technical standards (e.g. IP)
Sectoral	Training, skills development	Cybersecurity skills and best practices; CSIRTs; technical expertise and assistance	Market/commercial skills, e.g. operation of ICT technologies to provide digital services
Governance and diplomacy	Standards, norms, and regulatory frameworks	Data protection, cyber strategy, and cybersecurity policy development	Legislation for digital services and digital economy (e.g. e-commerce governance)
Table 4.6. Three dimensions of capacity building assistance for digital development based on author's review of the literature.			

Appendix B: Interviewee Details

From March 2021-September 2022, I conducted virtual interviews with European policymakers from the European Union External Action Service, the European Commission, EU CyberDirect, the European Union Institute for Security Studies, the Global Cyber Security Capacity Centre, and the UK National Cyber Security Centre. Interviews were semi-structured, ranging from approx. 30-60 minutes in duration, with questions tailored to individuals' professional experience with CCB. In line with the ethics and consent preferences of participants, I have not identified interviewees' specific roles. Ethics approval reference numbers are SSH_DPIR_C1A_21_005 and SSH_DPIR_C1A_22_008.

Interviewee Code	**Date**
1	03/5/2021
2	03/25/2021
3	04/15/2021
4	09/09/2022
5	09/15/2022

Article Acknowledgments

I would like to first thank my interviewees' generous support and contributions to my research. Further, I would like to warmly thank the journal editors, Myriam Dunn Cavelty, Nicole Jenne, and Yf Reykers for their kindness, encouragement, advice, and support, and the valuable suggestions by the article's two anonymous reviewers. Additionally, drafts of this article were presented at research-in-progress seminars at my department (Univ. Oxford), the Future of War Conference (2022) and the Hague Program for International Cyber Security (2023) in the Netherlands, and at the University of Surrey (2022). I am extremely grateful for the feedback and insights from colleagues in these seminars, workshops, and conferences, all of which have been instrumental for shaping the article. I am also grateful to my supervisors, several colleagues and friends at my department with whom I have had long discussions about weaponized interdependence and great power competition. Finally, this article would not have been possible without the generous funding provided by Nuffield College and the Economic and Research Council [ES/P000649/1].

Funding details

This work was supported by the Economic and Social Research Council [grant number ES/P000649/1], and by Nuffield College, University of Oxford.

Data availability statement

The author obtained approval for conducting research with human participants from the DPIR Departmental Research Ethics Committee (DREC) in accordance with the procedures laid down by the University of Oxford for ethical approval of all research involving human participants, and informed consent from all interviewees. Ethics approval reference numbers are SSH_DPIR_C1A_21_005 and SSH_DPIR_C1A_22_008. For interview dates, refer to the appendix. Due to the politically sensitive nature of the research and in line with interviewee consent, interview data cannot be made openly available.

Chapter 5: More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy[61]

Abstract

Despite the allure of 'European digital sovereignty' as an official European Union (EU) strategic objective, it remains unclear whether this discourse has driven concrete changes to EU external action policies, particularly those leveraging cyber instruments. This question is explored vis-à-vis three policies which have enabled the EU to pursue its digital sovereignty objectives in practice: the Cyber Diplomacy Toolbox, external capacity building (CCB) assistance, and the 5G Toolbox. Drawing upon extensive archival research and elite interviews, the paper finds that, while European digital sovereignty discourse influenced comprehensive changes for the 5G Toolbox process, it failed to drive policy changes to the Cyber Diplomacy Toolbox and external CCB assistance. To explore this variation, the paper considers institutional and ideational factors particular to EU external action over the 2017-2022 period. Overall, the study contributes to emerging debates about European digital sovereignty as it relates to cybersecurity instruments and to longstanding work on EU foreign policymaking.

Keywords: European security integration, EU foreign policy, digital sovereignty, sovereign power, cybersecurity

[61] A version of this article has been published. See Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy, 31*(8), 2250–2286. https://doi.org/10.1080/13501763.2023.2295523.

Introduction

European digital sovereignty has become a central reference point for the Union's approach to global affairs at a time of 'moving geopolitical plates' (Council of the European Union, 2022). While this discourse marks a striking rhetorical departure from its traditional eschewal of geopolitics in its foreign policy (Bellanova et al., 2022), it remains unclear whether it has driven concrete policy changes. Current literature has presented a fuzzy picture on this question: while some scholars have asserted that the discourse has served as an 'aggregator' for the Union's digital policymaking (ibid), others have cautioned that it conveys a 'false promise' for EU global leadership in artificial intelligence (Calderaro & Blumfelde, 2022). These findings raise questions as to whether Brussels' turn to 'European digital sovereignty' discourse has driven recent policy changes in EU external action. After all, the Union is known to suffer from a persistent capabilities-expectations gap in its foreign policy (Bendiek et al., 2020; Hill, 1993).

Particularly, while cyber instruments are touted as 'key enablers' for European digital sovereignty in EU strategic documents, the relationship between digital sovereignty discourse and concrete changes to cyber-relevant policies in the domain of EU external action remains unclear. Accordingly, this paper investigates the extent to which European digital sovereignty discourse has shaped concrete changes to policies within three established areas of EU action policy that leverage cyber instruments: EU common foreign and security policy (viz. the *Cyber Diplomacy Toolbox*), development cooperation (viz. *external cyber capacity building assistance programmes*), and trade and competition policy (viz. *the 5G Toolbox*). In keeping with the special issue framework (Falkner et al., 2023), the paper adopts a discursive institutionalist approach to characterize the relationship between discourse and policy change on the bases of extensive archival research and 20 elite interviews.

Analysis of these specific policy changes reveals remarkable variation: while European digital sovereignty discourse brought about comprehensive changes in the 5G Toolbox policy, it failed to drive the substantive changes towards digital sovereignty in the cases of the Cyber Diplomacy Toolbox and EU external cyber capacity building (CCB) assistance projects. Consequently, the paper explores how, in these cases, the varied influence of sovereigntist discourse has been shaped by institutional and ideational factors pertinent to EU external action policymaking. These findings contribute valuably to emerging debates about the effects of European digital sovereignty discourse on EU policy policymaking at large (Barrinha & Christou, 2022; Bellanova et al., 2022; Calderaro & Blumfelde, 2022). They also substantiate more longstanding EU Studies literature by demonstrating how the Union—despite its ongoing efforts to become a more ambitious, coherent, 'geopolitical' global player—continues to be mediated by institutional constraints, experiences of crises, and reputational considerations (Schmidt & Radaelli, 2004; Fisher Onar & Nicolaïdis, 2013).

The paper proceeds in four parts, beginning with its conceptualization of discursive and policy change and review of extant literature. Next, lays out its analytical framework and qualitative methodology, followed by an analysis of how European discursive change has emerged in EU external action. Then, it considers how this discourse has come to bear on three specific cyber-relevant policy areas of EU external action. Finally, it explores possible mechanisms that have influenced this relationship and concludes with contemporary and future implications.

European digital sovereignty discourse and EU policymaking

European digital sovereignty discourse has evolved over time to encompass a variety of diverse policy areas and 'layers' of meaning (Falkner et al., 2023). However, at its core, the discourse reasserts a claim to legitimate control over the Union's internal digital

environment (e.g. the 'Digital Single Market') and to shape its own destiny in the global digital domain—that is, its capacity to act as a global 'digital player' (Floridi, 2020). In other words, this claim has a dual dimension: the (internal) assertion of exclusive authority over a bounded socio-political space, its (external) legitimization through mutual recognition (Thomson, 1995). Therefore, *discursive change towards digital sovereignty* broadly entails an explicit deviation from existing policy discourses which construct the internet as entirely free from state involvement (Falkner et al., 2023).

In the case of the EU, discursive change towards digital sovereignty may also entail a discursive move from 'Member State *sovereignties'* to 'European sovereignty' (in the singular) relevant to the digital environment. From a realist perspective, the EU's assertion of a claim to 'sovereignty' could reflect a power multiplier logic for shaping global affairs as it demonstrates its capacity 'speak with one voice' (Wong & Hill, 2011) and to jointly act on behalf of its 27 Member States. Other scholars have pointed to how the EU's digital sovereignty claims have inherently sought to differentiate the EU from Others, including the United States, Russia, and China (Barrinha & Christou, 2022; Falkner et al., 2023). Recently, EU President Charles Michel positioned the EU's approach to digital sovereignty as somewhere '*between* an unregulated model and a state-controlled model [that] promote[s] a human-centric, ethics-based approach, that serves our citizens,' (emphasis added, Council of the European Union, 2021b). This further reveals the external/relational dimension to such discourse.

Separately, *policy change towards digital sovereignty* is conceptualized here as change towards 'control *over* the digital' domain and/or control *through* the digital: that is, 'the use of digital technologies for European (cyber)security governance' (Bellanova et al., 2022, p. 338). Policy instruments 'operationalizing' control over the digital include regulation and standard setting (Kuner, 2019); investment screening mechanisms; export

controls; industrial competition and R&D policy; government/public procurement strategies; cybersecurity; capacity building; and data protection/privacy tools (European Political Strategy Centre, 2019; Falkner et al., 2023). Given that the digital domain has both physical and virtual layers (some of which transcend territorial borders), control may manifest as *territorial* (as in 'territorial sovereignty') and/or *functional* authority over a (digital) space (Eudaily & Smith, 2008). Alongside the policy areas of AI and semiconductors, cyberspace has emerged as a domain through which digital sovereignty claims have been asserted and exercised by global actors, including the EU (Broeders et al., 2023; Chander & Sun, 2021; Calderaro & Blumfelde, 2022; Council of the European Union, 2021b; General Secretariat of the Council, 2022b; European Commission, 2022b).

This study focuses upon three cyber-relevant policy changes towards digital sovereignty in EU external action. These cases reflect the historically close relationship between the cyber and digital issues in official EU strategies/documents (see for example European Commission, 2010; 2014; 2016; 2017a; 2020d; 2022d). In the present day, 'cyber' is typically linked to 'network and information security' as an enabler of the 'digital' and as a 'fifth strategic domain of warfare' (Council Conclusions, 2015; Pawlak, 2018, p. 20; Barmpaliou & Pawlak, 2023, p. 93). By contrast, 'the digital domain' has come to be understood as a more encompassing socio-technical space, including the internet, digital technologies, 'space', the 'Digital Market', data, and an 'EU digital identity' (European Commission, 2021a).

Presently, Brussels understands cybersecurity as a key strategic 'priority', 'pillar', and/or 'cornerstone' for achieving European digital sovereignty (Bellanova et al., 2022; European Political Strategy Centre, 2019; General Secretariat of the Council, 2022b; European Commission, 2022b). For instance, the European Commission's current DIGITAL EUROPE programme asserts that cybersecurity is 'a prerequisite for Europe to

achieve digital sovereignty' (European Commission, 2023). Cybersecurity is considered to be a 'key policy area[] of the EU digital strategy' (Council of the European Union, 2021a), on account of the threats posed by cyberspace to the EU's strategic autonomy, 'at a time of growing dependence on digital technologies' (General Secretariat of the Council, 2022b, p.12). Accordingly, the EU's current cyber strategy (2020) establishes 'resilience, *technological sovereignty* and leadership' as the first out of three priority areas of EU global action, which will be supported by an 'unprecedented level of investment in the EU's digital transition over the next seven years' (emphasis added, European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2020, p. 4). Altogether, Brussels' current 'capabilities-based' approach towards the global digital domain relies upon cybersecurity as a key foundation and priority area, alongside AI and supercomputing (General Secretariat of the Council, 2022b, p. 35-37; see also European Commission 2022b, p. 7). The entanglement between cyber issues with digital sovereignty concepts in EU external action evinces a plausible connection between cyber-relevant policy changes and European digital sovereignty discourse.

Dynamics of change

How can we theorize about the relationship between discursive and policy change towards digital sovereignty in the domain of EU external action? A large body of work has demonstrated how discursive and policy changes have emerged as direct causes or consequences of each other (Schmidt & Radaelli, 2004). A discursive shift can spur policy change by altering established behavioural rules and acceptable standards for action (Finnemore & Sikkink, 1998). Alternatively, endogenous factors such as institutional complexity, feedback loops, identity considerations, and the interaction between various stakeholders can shape the relationship between discourse and policy change (Schmidt &

Radaelli, 2004). Exogenous factors, such as elites' experiences of transformative events can change policymakers' threat perceptions and introduce certain 'securitized' ideas into policy debates, thus informing future policy choices (Buzan & Wæver, 2003; Carrapico & Farrand, 2020; Christou, 2019). Elsewhere, Adler-Nissen and Gammelthoft-Hansen have argued that policymakers tend to invoke sovereignty when they perceive a loss of control over 'effective internal rule and freedom from external interference' (2008, p. 7). Thus, the concept of sovereignty can serve as a frame through which policymakers can justify and/or legitimize their policy decisions *ex post* (Walker, 2008). Indeed, scholarship on European digital sovereignty discourse has identified instances of the EU 'repackaging' earlier policies into sovereigntist frames, as seen by the policies proposed by the EU's 2020 Cybersecurity Strategy towards the Internal Market (Barrinha & Christou, 2022).

Other studies have pointed to the discourse's primary importance for EU identity (Monsees & Lambach, 2022; Csernatoni, 2022) and its use an 'aggregating concept' for policymaking (Bellanova et al., 2022). Separately, recent work on the relevance of European digital sovereignty discourse to the EU's AI policies has pointed to a disconnect between the EU's stated aims in AI and its actual capacity to ensure them. Despite its strong narrative, the Union 'has few tools to become a global leader in advancing standards of AI beyond its regulatory capacity' (Calderaro & Blumfelde, 2022, p. 415). Particularly, the Union's lack of 'hard' capabilities, a leading technological industry, and a coherent defence strategy have placed constraints upon its capacity to exercise digital sovereignty in the area of CFSP.

Complicating the matter further, scholarship on sovereignty and EU foreign policymaking has stressed that, rather than constituting a straightforward 'state-force-territory' relation (Barkawi, 2016), sovereignty claims uttered by the EU are unconventional: the product of a complex interweaving of different intergovernmental and supranational competences (Bartolini, 2006). In EU common foreign and security policy (CFSP), a key

dimension of EU external action, sovereignty is pooled between its Member States (Moravscik, 1998), which have been historically hesitant to cede control over their hard security, which can stunt the Union's 'hard' capabilities (Sliwinski, 2014). By contrast, the Commission enjoys exclusive competences over other 'softer' areas of external action: trade and economic security instruments. Therefore, speaking 'European digital sovereignty' in the context of EU external action is a potentially fraught, highly complex process involving 'plural' and/or 'mixed' sovereignties (Bellanova et al., 2022). Lastly, incoherence or institutional challenges in EU foreign policymaking could hinder the influence of discursive change on driving specific policy changes (Bendiek et al., 2020; Carrapico & Barrinha, 2017).

This scholarship suggests that, on the one hand, changing threat perceptions (tied to specific issue areas) might heighten the salience of European digital sovereignty discourse in some areas of EU external action rather than others, leading to variation in the discourse's significance across issue areas. On the other, assuming that sovereignty frames are expressed to reinforce and legitimize *existing* authoritative capacities (Adler-Nissen & Gammeltoft-Hansen, 2008), the EU's existing areas of strength and material competences (namely trade and economic security) would be highly conducive for digital sovereignty discourse to influence concrete policy changes as opposed to other domains (such as the consensus-based, intergovernmentalist CFSP). Alternately, if European sovereigntist discourse is largely invoked to legitimize the EU's policies *ex post* (Barrinha & Christou, 2022)—perhaps for the purposes of identity construction (Csernatoni, 2022)—the discourse might not decisively influence *ex ante* policy changes either (Schmidt & Radaelli, 2004).

In sum, extant scholarship suggests that four distinct causal processes might underly the relationship between sovereigntist discourse and policy changes in EU external action:

1) discursive change has driven policy change; or

2) vice versa; or

3) changes are driven by a policy-discourse feedback loop; or

4) changes in discourse and policy have been driven by other factors.

This paper examines whether discursive change towards European digital sovereignty has driven policy changes in the same direction (*dynamic 1*) and the extent to which variation in this outcome is observable across three cyber-relevant policy changes. However, the scholarship reviewed above is testament to the fact focusing upon *dynamic 1* vis-à-vis three cases of EU external action policy change is inadequate for advancing 'complete' explanations about the policy change process as a whole (Ebbinghaus, 2005). After all, discourse 'is one among several factors involved in policy change' (Schdmit & Radaelli, 2004, p. 189). Nonetheless, exploring *dynamic 1* lays the basis for future inference about whether policy change has instead driven discursive change (*dynamic 2*) in these cases, whether there exists a causal feedback loop (*dynamic 3*), or whether additional factors have shaped both discursive and policy changes (*dynamic 4*). It also contributes to scarce literature which examines the relationship between the rise of European digital sovereignty discourse and significant changes to EU external action policies.

Analytical Framework

Reviewing extant literature thus raises two fundamental questions: *when* and *how* does discourse matter for policy change? For the purposes of this paper, these questions are explored in line with the discursive institutionalist approach (Schmidt & Radaelli, 2004) and the framework outlined by this special issue (Falkner et al., 2023), which underscore the importance of discourse within a particular institutional context. To influence the policy change process, Schmidt and Radaelli argued that 'the story the discourse tells and the information it provides must also appear sound, the actions it recommends doable, the

solutions to the problems it identifies workable, and the overall outcomes appropriate' (2004, p. 201).

Therefore, to infer whether a discourse has driven a particular policy change, the paper relies upon the following criteria: *sequencing, significance,* and *distinctiveness.* These criteria are examined with respect to the *explicit* use of digital sovereignty discourse in EU external action policies. This assumes, coherent with the discursive institutionalist approach, that 'speaking of change […] rather than just thinking it, is key to explaining the actions that lead to major policy transformations,' (Schmidt, 2011, p. 106).

As represented by Table 5.7 below, sequencing is critical: evidence of discursive change must have occurred *prior* to the policy change for it to affect the outcome. Second, building on Falkner et al.'s (2023) framework, the discourse must be *significant,* meaning that its core ideas are central, relevant, and applicable to the policy in question. A particular discourse is *relevant* when there are identifiable problems and challenges that sovereignty discourse is expected to resolve vis-à-vis a particular policy, and *applicable* when a policy specifies *how* sovereignty discourse solves these challenges (ibid, pp. 4-5). Third, departing from Falkner (2023) and colleagues, I explore the relative *distinctiveness* of concepts *within* European digital sovereignty discourse. Since discourse constitutes a web of 'policy ideas and values' negotiated and contested by policy actors (Schmidt & Radaelli, 2004, p. 184), policymakers might deem some discursive concepts more significant than others for a given policy issue, contest the meaning of competing concepts within a discourse, or conflate the meaning of several similar concepts. Therefore, to establish a concept's *distinctive* influence over a given policy change, it must have exerted an *empirically distinguishable* effect on policy changes from other competing ideas (Schmidt, 2002, p. 219).

Based on these criteria, several distinct types of discursive-policy change relationships are possible within the paper's parameters (see Table 5.7). The causal role of

discursive change vis-à-vis policy change can be inferred by establishing temporal sequencing as a necessary test. Separately, Falkner and colleagues outlined two dynamics of discursive and policy change (agnostic of their causal relationship) relevant to this paper. First, *comprehensive change* embodies a process whereby digital sovereignty discourse is a 'central and positive discursive reference point' and policy change towards sovereignty is 'significant' (Falkner et al., 2023, p. 22). Second, when discursive change fails to satisfy the criterion of significance yet the *policy change* is significant, this relationship can be characterized as *inconspicuous change* (ibid). Lastly, my paper introduces a third dynamic to Falkner and colleagues' framework: *(in)distinctive* change, whereby digital sovereignty discourse is a positive and applicable reference point, but the discursive *concept* in question (e.g. 'European digital sovereignty') is (not) distinctive vis-à-vis the policy change. Thus, *indistinctive* change occurs when a discursive concept is substitutable or conflated with another prominent competing concept, such as 'technological sovereignty', or 'strategic autonomy' as opposed to 'digital sovereignty'. Altogether, these analytical criteria will be used to empirically identify the character of discursive-policy change relationships in EU external action.

Level of analysis	**Criterion**	**Observed?**	**Relationship to policy change**
European digital sovereignty *discourse* as a core set of ideas	**Temporally prior to policy change?**	**Yes**	Plausible causal role (necessary, not sufficient)
		No	Does not drive policy change
	Significance?	**Yes**	*Comprehensive*
		No	*Inconspicuous*
Individual 'European sovereignty' *concepts* in policy discourse	**Distinctiveness?**	**Yes**	*Distinctive*
		No	*Indistinctive*

Table 5.7: Falkner et al.'s framework (2023) with my modifications (in grey)

Methodology

As outlined above, the paper's aims are twofold: to characterize the relationship between European digital sovereignty discourse and three specific cyber-relevant policy changes in EU external action, and to identify the temporal sequencing of European digital sovereignty discourse vis-à-vis a given policy change. To trace the role of discourse in these policy changes**,** the paper conducts a discourse analysis of EU digital sovereignty discourse. Next, it undertakes an abductive 'explaining-outcome' process tracing approach (Beach & Pedersen, 2019) focused upon how the discourse came to bear upon three specific cases of EU external action which exemplify significant policy change towards sovereignty in practice: the Cyber Diplomacy Toolbox, EU external cyber capacity building (CCB) programmes, and the 5G Toolbox.

First, the paper constructed a genealogy of the emergence of European digital sovereignty discourse in official EU external action policy discourse based upon an interpretive-qualitative analysis of textual sources and elite interviews (Schwartz-Shea & Yanow, 2012; Schmidt, 2011). Discourse analysis is important for exploring the *sequencing* of discursive change vis-à-vis the paper's cases of policy change, and for understanding the process of ideational convergence between 'digital' and 'cyber' issues into EU external action policy discourse over time. Therefore, it is also valuable for assessing whether digital sovereignty could be *plausibly* relevant to the three cases of policy change in the paper.

To do so, the analysis engaged in intertextuality, or the process of situating texts within and against other texts to reveal how one particular source (e.g. a strategy document) is embedded within the broader political and social discourse (ibid). This analysis also elucidated key constitutive concepts of European digital sovereignty discourse and policy contexts whereby the discourse was officially absent (Schwartz-Shea & Yanow, 2012). To this end, the data were analysed for how they represented policy issues as *particular* types of problems (Bacchi & Goodwin, 2016) to examine the extent to which digital sovereignty

discourse was understood to be *relevant* and/or *applicable* to a particular policy instrument or issue.

Relying upon the EURLEX database a starting point, I reviewed the corpus of documents pertinent to the overlapping areas of EU cybersecurity policy, digital policy, and EU external action over the 2010-2022 period. This timeframe coincides with the inception of the EU's diplomatic branch, the European External Action Service (EEAS). Altogether, over 100 relevant primary source documents (*inter alia* digital and cyber strategies, Staff Working documents, Council *Conclusions,* EU regulations, and European Parliament debates) were analysed for the presence/absence of European sovereignty discourse and its relationship to relevant policy changes. Working abductively, I examined documents through a temporalized mapping technique to identify the relevant institutions and sites of discourse (Clarke, Friese, & Washburn, 2015). This in turn facilitated exposure to the perspectives of the many policy actors involved in shaping and disseminating EU digital sovereignty discourse (ibid). The analysis largely concentrated upon the EU level, with the Union's external action policymaking developed 'with reference to values and principles that are seen as *particular* to the Union' (Sjursen, 2011, p. 1089). This level of analysis captures the bulk of developments in EU cyber and digital policy post-Lisbon Treaty in EU external action (Laurer & Seidl, 2021; Timmers, 2018; Pawlak et al., 2018; Trimintzios et al. 2017, p.5). However, this approach does not preclude the examination of intergovernmental discursive struggles over the meaning of EU digital sovereignty at the horizontal level (e.g. between various Committees and/or Representatives in the Council of the EU) or vertical levels (e.g. between Brussels and Member States).

To corroborate my document analysis, I conducted 20 elite interviews (Appendix A),[62] comprising 15 EU officials and five policy experts from bodies which have influenced the development of the EU external action policy changes of interest. Interviewed policymakers were current or former practitioners from various divisions within the European Union External Action Service (EEAS), the European Commission, and the Council of the EU. In this group, five interviewees were current or former heads of division, directors, or members of Brussels' executive cabinet, and several interviewees were career diplomats, with professional experience in multiple relevant EU bodies or as Member State representatives. Collectively, their professional experience exhausted the 2010-2022 timeframe and spanned the development of the key three policy changes relevant to the analysis. Furthermore, five policy experts were interviewed from consultative or EU-funded bodies and think tanks, such as EU Cyber Direct, the European Union Institute for Security Studies, and the Council of Europe. Interviews were semi-structured and 30-60 minutes long. Questions were tailored to individuals' professional experience and their involvement in policymaking, including their understanding of which concepts and ideas are/were 'most important' to the policy in question, and the key factors (including events) that have influenced the EU's external action policymaking.

Examining three policy changes towards sovereignty

Next, in line with its analytical criteria (Table 5.7), the paper traced how this discourse came to bear upon three cases of *significant* policy change towards digital sovereignty in

[62] The author obtained ethics approval for conducting research with human participants from the appropriate institutional review board and informed consent from all interviewees. Ethics approval reference numbers are SSH_DPIR_C1A_21_005 and SSH_DPIR_C1A_22_008. For interview dates, refer to the appendix. Due to the politically sensitive nature of the research and interviewee consent, interview data cannot be made openly available. However, the archival sources used by the study are openly available, accessible at the EURLEX database and as noted in the reference section of the paper.

EU external action: the Cyber Diplomacy Toolbox, EU external CCB programmes, and the 5G Toolbox. Recall that the paper theorized four possible relationship dynamics between discourse and policy change (dynamics 1-4), including the possibility that discourse drove policy change (dynamic 1). While the paper concentrates upon dynamic 1, its approach does not aim to evaluate the general validity of one causal mechanism 'but rather to identify the main drivers' behind the shared outcome of *significant change towards sovereignty* in three specific cases (Beach and Pedersen, 2019, p. 282, in Haroche, 2022). Accordingly, throughout its analysis, the paper remains open to other causally relevant factors, such as ideational and institutional factors, which could have contributed to the outcome(s) of significant policy change towards sovereignty. This exploration paves the way towards developing a more holistic understanding of the relationship between discourse and policy change in these specific cases (see Haroche, 2022 for a similar approach).

Notably, as EU external action spans multiple encompassing policy areas, and 'cyber' and 'digital' are transversal issues (Pawlak, 2018), the paper's three cases are not representative of all significant policy changes towards digital sovereignty. Therefore, the relationship between digital sovereignty discourse and other cases of policy changes may be different than that of the cases selected by this study. Nevertheless, as I outline below, these cases are worthwhile to examine as they remain strategically important for EU external action and its aims to achieve European digital sovereignty in practice. Furthermore, the cases represent diverse aspects of EU external action in terms of their policy scope and instrumentation.

Significant policy change is observable when 'policies move *substantially* in either the *degree*, *form*, or *direction* towards more control of the digital, be that quantitatively or qualitatively' (Falkner et al, 2023, p. 9). As sketched by the below figure (Figure 5.1), the Cyber Diplomacy Toolbox, external CCB projects, and the 5G Toolbox cases fulfil this

criterion and temporally overlap with the mainstreaming of European (digital) sovereignty discourse into EU external action policy.

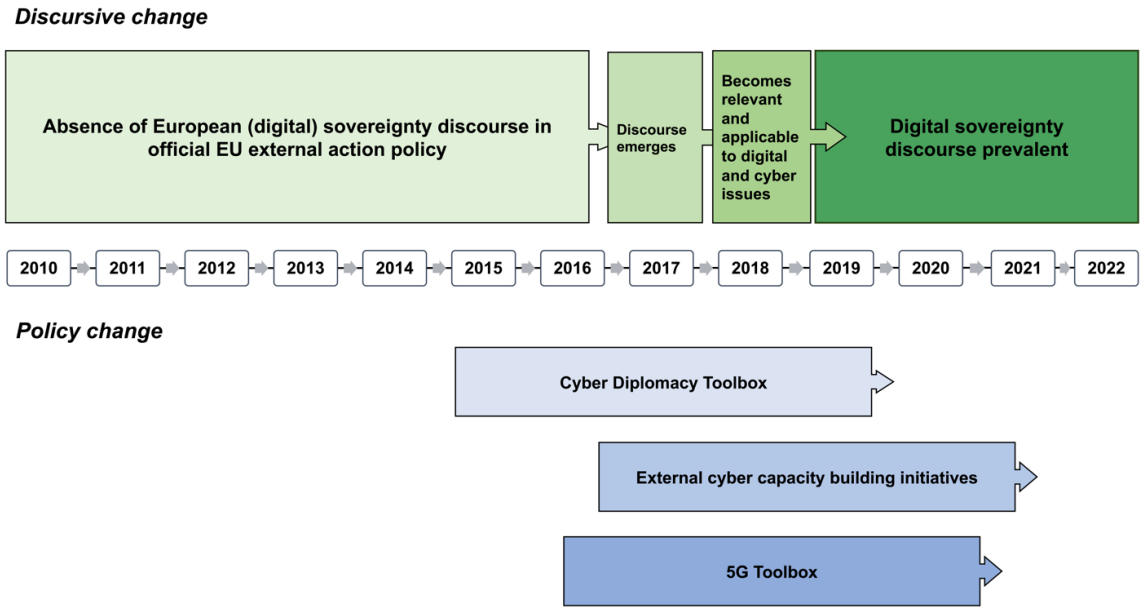


Figure 5.17. Overlap between discourse and policy change towards sovereignty in EU external policy.

Relevant for the paper's timeframe, cyber and digital diplomacy matters were not siloed as 'visibly' separate issues in EU policy up until June 2022 (Interviewees I,T; General Secretariat of the Council, 2022a). Furthermore, 'the priority *actions'* for digital diplomacy—as distinct from cyber diplomacy—were only adopted in June 2023 (emphasis added by author, General Secretariat of the Council, 2023). Throughout this period, policy portfolios were divided between the EEAS, tasked with cybersecurity and defence matters, and the Commission's DG CONNECT, which is held responsible for AI, 5G, and other critical digital technologies (Interviewee I). Nonetheless, the Commission and the EEAS still closely coordinate on EU external action policies, especially those pertaining to cyber and digital issues given their transversal nature (Interviewees I,T). While this development demonstrates the growing sophistication of EU external action policy towards the digital domain, it also highlights the relatively high significance of cyber diplomacy for the EU's

global approach to digital governance up until that point (Latici, 2020), including in multilateral fora and public-private partnerships (Carrapico & Farrand, 2020; Pawlak & Barmpaliou, 2023).

As instances of significant policy change towards digital sovereignty, the Cyber Diplomacy Toolbox, CCB assistance programmes, and the 5G Toolbox involve diverse instruments which enable both the internal and external dimensions to sovereign control over the digital (Thomson, 1995), summarized in Table 5.8. The Cyber Diplomacy Toolbox, by enabling the Union to 'make full use of measures within the Common Foreign and Security Policy' in the global cyber and digital domains (Council of the European Union, 2017), significantly increased the Union's authority to coercively act in the digital domain. The 2019 update enables the EU to punish (and deter) negative interference in the Union's Digital Single Market, thus delineating (un)acceptable behaviour in global cyberspace from the EU's perspective. Next, through significant changes in the orientation and funding of external CCB initiatives, the EU has been able to influence the global digital environment through spreading EU values and standards to strategically important regions (Renard, 2018; Prontera & Quitzow, 2022). By exporting EU values and practices to external locales, these developments reflect the 'security-development' nexus in EU external action policy (Pawlak & Barmpaliou, 2017; 2023) and they signal Brussels' ambitions to become a global standard-setter and legitimate geopolitical actor (Bradford, 2020; Bialasiewicz, 2015; Manners, 2002). Exporting the EU's preferred norms and regulations have been a way for the EU to project power and exert control over the global digital environment in the absence of mutually agreed-upon standards for behaviour, including in the area of cybersecurity, data protection, and lethal autonomous weapons (European Commission, 2022c; Cremona & Scott, 2019; Calderaro & Blumfelde, 2022). Lastly, the 5G Toolbox seeks to reduce the Union's vulnerabilities to dependency on foreign entities for its critical digital infrastructure

by enhancing Brussels' capacity to act in the Digital Single Market and outlining a European approach to 5G global governance (Monsees & Lambach, 2022). Altogether, these cases relate to four out of six dimensions of EU external action: the CFSP (the Cyber Diplomacy Toolbox); development cooperation and economic, financial and technical cooperation with non-EU countries (external CCB programmes); and trade policy (the 5G Toolbox).

Significant policy change towards digital sovereignty	**Dimension of external action**	**Type of control over the digital**
Cyber diplomacy toolbox	CFSP	Internal- coercive measures External – promoting EU approach to legitimate cyber behaviour
External CCB initiatives	Development cooperation and economic, financial and technical cooperation with non-EU countries	External- regulatory, normative (conditionality instruments) and infrastructure investments
5G Toolbox	Trade and competition policy	Internal - control over foreign interference External – considered EU 'standard' for 5G governance

Table 5.8. Summary of case characteristics.

Furthermore, these cases have been touted as strategically important for EU external action, including for the EU's diplomatic objectives (General Secretariat of the Council, 2022a). The EU's contemporary *Strategic Compass* names the Cyber Diplomacy Toolbox as a crucial aspect to securing the EU against emergent threats and challenges (General Secretariat of the Council, 2022b, p. 22) and the primary 'international aspect' for EU cybersecurity, guiding the EU's diplomatic response to cyber threats to the digital domain (European Commission, n.d-a; General Secretariat of the Council, 2019). Separately, external CCB has high strategic importance for the EU's cyber diplomatic efforts (Council of the European Union Presidency, 2016), for 'strengthen[ing] the [EU's] approach to strategic cooperation with its Eastern and Southern Neighbourhoods' (General Secretariat

of the Council, 2022b, pp. 39-44). Externally, the 5G Toolbox remains the 'standard' model for promoting the Union's approach to the securing critical infrastructures to its partners (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2020). As I will detail below, the EU's explicit turn towards digital sovereignty emerged after a decade of significant global events, rapid technological innovations, and transformations to the Union's internal environments.

Discursive change

Digital sovereignty has been linked to 'diverse measures, guiding principles, and the empowerment or constraint of different actors' at the global, supranational, and regional levels, including cybersecurity, AI, supercomputing, semiconductor chips (Falkner et al., 2023, p. 3; Floridi, 2020). In the European context, scholars have argued that it emerged from French and German discourses 'uploaded' to the EU level (Moerel & Timmers, 2021), while others have emphasized the influential role of Council President Charles Michel (Barrinha & Christou, 2022). Particularly in the domain of EU external action, global security crises over the 2014-2020 period, policy mainstreaming, and changing perceptions about the EU's role as a geopolitical actor were important for bringing about a discursive shift towards sovereignty in EU external action. Here, European digital sovereignty discourse rose to prominence over a three-year period, peaking in popularity during the von der Leyen Commission in 2019. Since 2019, three concepts have primarily constituted this discourse: European digital sovereignty, technological sovereignty, and (open) strategic autonomy.

At the time of the EEAS' inception in 2010, European digital sovereignty discourse was out of bounds for EU external action. While the EU's first *Digital Agenda* (2010) emphasized the importance of cybersecurity for preserving a European 'digital way of life', dissensus at both the horizontal and vertical governance levels about the scope of the Union's

role in cyberspace precluded *European-wide* sovereignty to emerge in EU discourses (Zanders, 2009; European Union Committee, 2010; European Commission, 2010, pp. 5, 27). Accordingly, the EU's first *Cybersecurity Strategy* (2013) advanced a modest, inward-looking orientation and an ambiguous approach to the EU's role as a global cyber actor.

However, this hesitancy was later shattered by transformative crises over the 2013-2016 period and by the realization that 'the EU is lagging behind in the development of both its digital infrastructure and innovative enterprises' (Reding, 2016, p.1). In global affairs, the 2014 Ukraine crisis, the 2015 refugee crises, and shaky transatlantic relations after President Trump's election in 2016 (among others) exposed the uncertain and evolving character of the global security environment and the imperative for an assertive European global approach (Lutz & Karstens, 2021; Interviewees A,C,D). Meanwhile, the Snowden revelations about the American government's global digital surveillance operations fuelled the push for a European approach to data protection and privacy (Coyne, 2019). While 'the national ministers in the Council dragged their feet' until 2016 (Reding, 2016, p. 5), the later release of the *General Data Protection Regulation* (GDPR) would be heralded as one of the EU's 'greatest' achievements in data protection (Kuner, 2019). While European digital sovereignty discourse was absent in official discourse announcing its release (Laurer & Seidl, 2021), Viviane Reding (writing as a Member of the European Parliament at the time), argued that the GDPR helped to ensure European digital sovereignty over citizens' data (Reding, 2016).

Yet, until the 2016 release of the *Global Strategy for the European Union* (hereafter 'EUGS'), European sovereignty discourse had not permeated official EU external action policy. The EUGS advanced a vision for the EU to become a 'forward-looking cyber player' to assure European *strategic autonomy* (European External Action Service, 2016, emphasis added, p. 42). Significantly, it paved the way for the uptake of European sovereigntist

discourse *and* the mainstreaming of 'digital' and 'cyber' aspects in EU external action policy. Shortly thereafter, the 2016 *Council Conclusions* highlighted the need to 'properly mainstream' digitalisation across 'all policy areas, including in the EU's development and foreign policies, while addressing cyber challenges…' (p. 2). In turn, the Commission's 2017 *Reflection Paper on European Defence* noted that greater EU-level cooperation and an enhanced EU-specific role would strengthen Member States and make them 'more sovereign' (p. 11). Echoing the sentiments of the EUGS, the 2017 *Paper* also 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' (ibid, p. 7).

This general notion was later reflected by the EU's updated cybersecurity strategy, *Resilience, Deterrence and Defence,* released in September 2017, which stressed 'due diligence and state responsibility in cyberspace' and for the EU to achieve 'greater resilience and strategic autonomy' (p. 18). By 2018, EU external action policy discourses had established an overt link between the ideas of *European sovereignty, responsibility, resilience,* and *strategic autonomy*, including vis-à-vis the cyber and digital domains (e.g European Commission, 2018b; n.d.-b). 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 (Interviewee C). Three concepts emerged to constitute the core of European digital sovereignty discourse at the domain level: *strategic autonomy* and *European digital* and/or *technological sovereignty*. These notions entangled with older EU external action concepts (such as *responsibility, resilience* and *leadership*) to comprise a new orientation under von der Leyen's 'geopolitical Commission'.

As one interviewed official put it, while the process of discursive change 'didn't happen overnight […] the pace changed with the von der Leyen Commission' in 2019

(Interviewee K), leading to Brussels' widespread adoption of an explicitly geopolitical, 'state-centric sovereignty lexicon' (Bellanova et al., 2022, p. 339). Brussels' evocation of European digital sovereignty emerged at a time when such assertions have become increasingly 'in vogue' at the global level, including in the case of Russia and China (Chander & Sun, 2020). The Union's changed geopolitical perceptions about the global environment raised the salience of sovereignty issues in both national and supranational contexts (Interviewee C; Monsees & Lambach 2022). The COVID-19 pandemic further reinforced the applicability of 'European digital sovereignty' to EU external action as it underscored the Union's critical dependencies on digital services and their vulnerability to weaponization (Interviewee M; Lipscy, 2020; Pawlak & Barmpaliou, 2023). The rise of powerful private actors as digital service providers and their control over critical infrastructure (Calderaro & Blumfelde, 2022), as well as companies' exploitation of data for economic purposes (Zuboff, 2019) fuelled the perception that the EU's security and digital capacity were becoming critically reliant upon foreign actors and private intermediaries. Additionally, the Biden Administration's openness to European strategic autonomy has been credited as an enabler for the broad uptake of the discourse (General Secretariat of the Council, 2022; Interviewee C).

Altogether, digital sovereignty discourse was increasingly framed as the solution to multiple concerns: the cybersecurity risks of using Chinese technology for critical European infrastructure (NIS Cooperation Group, 2019), the increasingly outsized role of foreign tech giants in shaping the European digital ecosystem, including data and AI (Carrapico & Farrand, 2020), the socio-economic and geopolitical risks of competitive US-China dynamics (European Commission, 2021b; European Commission & HR/VP, 2019), and the lack of a 'level playing field' for European technology firms in foreign markets and in global digital value chains (European Commission, 2020a; Interviewee D; General Secretariat of

the Council 2020, p. 4). These concerns reinforced the idea, in one EU official's words, 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' to maintain European sovereignty in the digital domain (Interviewee A). To this end, the EU's 2020 strategy, *Shaping the Digital Future,* has underlined the importance of EU leadership in digital technologies and cybersecurity and envisaged an unprecedented level of investment in the EU's digital transition' (European Commission 2020d, p. 3).

Relationship to policy changes

This section probes the relationship between European digital sovereignty discourse and three policy changes: the Cyber Diplomacy Toolbox, external CCB initiatives, and the 5G Toolbox, discussed in turn below.

The Cyber Diplomacy Toolbox

In High Representative (HR/VP) Josep Borrell's words, the updated Cyber Diplomacy Toolbox is the 'EU autonomous cyber-sanctions regime', which 'send[s] a message to the world that we have the tools to protect ourselves, and the resolve to use them,' (European External Action Service, 2020). Currently in force, it enables the Union to exercise further control over its internal security and cyber threats to the Digital Single Market 'through imposing, if necessary, restrictive measures on select entities' (Latici, 2020). The Cyber Diplomacy Toolbox has been important aspect to the EU's cyber diplomacy efforts, 'to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace, and effective global digital governance' (ibid, 2020, p. 1). However, for all its significance in EU external action towards the digital domain, European digital sovereignty discourse was not relevant or applicable to the Toolbox update process.

It should be noted that the process of updating the Cyber Diplomacy Toolbox was set in motion in 2017, two years before European sovereigntist discourse became widely popularized in Brussels' official discourse. Nonetheless, as the duration of the Toolbox's creation (2017-2019) covers the period of sovereignty's mainstreaming into EU external action policy, it is possible that the discourse could have penetrated the policy process.

Indeed, while the *EUGS* had laid the basis for the EU to engage 'in cyber diplomacy and capacity building with our partners […]' to assure European strategic autonomy (2016, p. 42), there was no apparent embrace of digital sovereignty concepts in Cyber Diplomacy Toolbox discussions. The *Council Conclusions on Cyber Diplomacy* established the need for a concerted European approach to cyber diplomacy and the Council began to consider introducing restrictive measures to the Toolbox in June 2017 (Council of the European Union, 2017). In track with other EU strategy documents at the time (Juncos, 2017), early debates about a coordinated EU approach to cyber diplomacy concerned issues of resilience and critical digital infrastructures. At that point, the official rationale for incorporating restrictive measures to improve the Union's security and address the growing number of 'malicious cyber activities' in cyberspace (General Secretariat of the Council, 2017, p. 4).

Thus, despite the Council's growing awareness about the rapidly evolving context of cybersecurity and defence (Council of the European Union, 2016, p. 2), the Commission had to 'persuade' Member States to move beyond a narrow focus on national security resilience issues to considering cross-border risks that required a collective European approach (Interviewee K). In September 2017, the Commission penned a joint communication stressing that 'the scale and cross-border nature of the threat make a powerful case for EU action,' whereby state actors 'are increasingly meeting their geopolitical goals' through the use of 'more discreet cyber tools' including the basic 'functioning of our democracies, our freedoms, and our values'—and therefore, into the

sovereign control of Member States (European Commission & HRVP, 2016). Commission President Jean Claude Juncker emphasized that, 'Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks' (State of the Union, 2017), underscoring the relevance of 'cyber' for EU internal and external security. The following year, Juncker would go on to outline his vision of 'European sovereignty', urging Member States that, 'together we can plant the seeds of a more sovereign Europe' (State of the Union, 2018).

One year later, the Council's *Decision* 2019/797 laid out the legal framework for the Toolbox's array of targeted restricted measures, which 'also allows for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations.' In keeping with earlier discourse on the Toolbox, the document reiterated the importance of addressing 'malicious cyber activities' through a comprehensive 'joint EU diplomatic response.' Moreover, the Council noted that the Cyber Diplomacy Toolbox 'contributes to conflict prevention, cooperation and stability in cyberspace by setting out measures within the CFSP, including restrictive measures, that can be used to prevent and respond to malicious cyber activities' (ibid)—omitting 'European digital sovereignty' discourse yet again.

Therefore, despite multiple Commission publications about the geopolitical context, the necessity for 'European sovereignty', and the risk of foreign interference into EU internal security,

> 'The Cyber Diplomacy Toolbox work wasn't framed around sovereignty, in part because we were dealing with *national security* challenges and had to engage member states to work together […] Telling them this was about European sovereignty wasn't necessarily the best way of doing that. (Interviewee K, 2022).'

Conversations about the Toolbox's revision thus remained 'very pragmatic and practical' (Interviewee K). Member States' awareness of their vulnerability to cross-border security risks was crucial for engaging policymakers to work together and push through the Cyber

Diplomacy Toolbox update, but it did not extend to explicit recognition of 'European sovereignty' concepts (Interviewees J, K).

Notably, while the 'Cyber Diplomacy Toolbox work wasn't framed around sovereignty' during its creation, the Council later cited it as an important part of the EU's 'progress' towards strengthening European technological and digital sovereignty (General Secretariat of the Council, 2022a). Therefore, this case is exemplar of *inconspicuous* change, whereby the discourse lacked applicability and significance throughout the policy process despite its *ex post* association.

External Cyber Capacity Building

External or cooperative CCB assistance is generally 'an umbrella concept for all types of activities (e.g. human resources development, institutional reform or organisational adaptations) that safeguard and promote the safe, secure and open use of cyberspace', whereby cyberspace is considered to be a part of the digital environment (Pawlak, 2014, 6; in Collett, 2021). Throughout the period of discursive change towards sovereignty, EU external CCB initiatives underwent significant changes in terms of their financial, strategic, and political remit towards greater control over the digital. However, alike the *Cyber Diplomacy Toolbox,* European digital sovereignty discourse was largely absent in the process of bringing about these changes, which renders the discourse-policy relationship *inconspicuous*.

With the new 'joined up approach' heralded by the EUGS in 2016, CCB projects began to enjoy elevated diplomatic and strategic value in EU policy (General Secretariat of the Council, 2016; Council of the European Union Presidency, 2016). Citing the 'borderless' nature of threats in cyberspace, the Council called for 'enhancing cyber capacity building

action under external assistance instruments,' (Council of the European Union Presidency, 2016, p. 3; see also European Commission 2018b, p. 4).

Following their reorientation from cybercrime to become more inclusive of security and defence, external CCB initiatives have aimed to transform the EU's global security environment in line with Brussels' values and strategic interests (European Commission, 2022b). To this end, external CCB projects have promoted the implementation of 'Made in Europe' solutions (European Commission, 2017a, p. 15) to partner countries, including the 5G Toolbox and the GDPR. Such initiatives rely upon conditionality, such that EU funding *and* EU values are exchanged for partnership with third countries (Interviewee F; Renard, 2018). Indeed, EU Kenya has been regarded as the model of success, which recently adopted the EU's 'GDPR-like' data privacy legislation into its national cybersecurity policy framework (Interviewee E). Overall, these initiatives have extended Brussels' influence over the governance of the global digital domain by nudging the development of third countries' national regulations towards EU-approved global cyber rules (Interviewees E, G). Notably, whereas *cyber* capacity building initiatives attained a higher strategic value with the release of the EUGS, there was relatively little emphasis on *digital-specific* initiatives under the Digital4Development framework in this regard. As the Commission noted in 2017, 'EU support on digital technologies and services in development cooperation has focussed on financing digital components of projects in *other* focal sectors' (emphasis added by author, ibid, pp. 8-10).

Indeed, while the importance of incorporating 'cyber resilience elements in projects dealing with critical infrastructures' was initially emphasized in the 2017 Digital4Development framework due to the 'cross-sectorial nature of digitalisation' (European Commission, 2017a, p. 13), this approach was enhanced through the introduction of a new blended financial instrument, the NDICI, 'for the Digital Decade'. Notably, the

NDICI framework was designed to enable the EU respond to its 'foreign policy needs and priorities' through merging various financial instruments (European Commission, 2018a). Accordingly, the restructuring of external CCB from the IcSP framework to the new NDICI instrument expanded the programmes' financial remit to include building external partners' *infrastructural* capacities (European Commission, 2021c, 2022a). As one interviewee observed, whereas there had once been a 'conscious exclusion' of infrastructure in EU external CCB funding, this dimension has become a priority (Interviewee H). Thereafter, the EU has recently financed submarine cables in Latin America and various internet connectivity programmes in Africa by means of its 2021 Global Gateway initiative, which incorporates capacity building as a main tool, including CCB (European Commission, 2021c, 2022a; Pawlak & Barmpaliou, 2023). By establishing a stronger EU presence in the development and governance of global ICT infrastructures, such a change allows for further EU control *over* and *through* the global digital domain.

Despite enabling greater EU control over the global digital domain in practice, European digital sovereignty discourse has remained largely absent in policy updates to external CCB. Notably, the discourse was not observably relevant and/or applicable to the Digital4Development framework's reorientation in 2018 towards a greater emphasis on the strategic value of cyber capacity building (Pawlak, 2018). Furthermore, policy changes which took place during/after 2019—such as the expansion of CCB to include infrastructural capacity building—have not been expressly linked to European digital sovereignty goals.

Rather, policy continuities, particularly the emphasis placed on exporting the EU governance model and adopting a geographically targeted approach to development, remain priorities in 2022 (see also Prontera & Quitzow, 2023). As the Council reasoned in 2020, '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,' (emphasis added by author, p. 13). Furthermore, while European digital sovereignty was rarely articulated by interviewed policymakers in this context, the concept of 'responsibility' was highlighted as a key motivating reason for CCB policy changes (Interviewees A; F, 2021), demonstrating discursive continuity with the *EUGS*. As one interviewee (A) expressed, the EU decided to undertake a strategic approach to its CCB programmes in part because 'we [the EU] were asked also by international partners to take more responsibility of what we do and how we do it.'

Nonetheless, European sovereigntist discourse has not been *entirely* absent from these policy developments. The 2018 update of external CCB guidelines emphasized CCB's significance for fulfilling the objective of *strategic autonomy* (General Secretariat of the Council, 2018). Further, one interviewee asserted *ex post* that digital development cooperation (through EU external CCB initiatives) remains a key pathway to promote European digital sovereignty abroad (Interviewee I). Similarly, the 'Digital4Development hub', launched in 2020, has increasingly framed '*digital* capacity building' as being strategically important (European Commission, n.d.-b) with a decreased emphasis on 'cyber' capacity building (although external CCB initiatives are still considered key enablers; see Pawlak & Barmpaliou, 2023). This suggests that EU external CCB programmes and their objectives are being repackaged under the mantle of European digital sovereignty discourse. However, when official 'Digital4Development hub' documents have explicitly referenced digital sovereignty, it has mostly been in reference to the 5G Toolbox (ibid). Overall, the specific way(s) in which *concrete changes* to EU CCB programmes have been influenced by European digital sovereignty discourse has not been explicitly laid out in official documents. Based on the meagre evidence available, the relevance and applicability of European sovereignty discourse is negligible and conceptually *indistinguishable* from that of strategic autonomy, thus exemplifying *inconspicuous change*.

The 5G Toolbox

Unlike the previous two cases, European digital sovereignty discourse was applicable and relevant to the 5G Toolbox policy change process, therefore exemplifying *comprehensive change*. In 2015, concerns emerged about the foreign acquisition of strategic digital technologies on the EU internal market, particularly in terms of the EU having 'critical dependencies' on foreign suppliers (Interviewees A, I). This was particularly cogent to 5G networks, which facilitate the 'Internet of Things' through connecting key domains—including political, strategic, military, economic, industrial dimensions—at the personal, local, national, and international levels (European Commission, 2022e). Accordingly, the Commission's *5G Action Plan* offered the first serious step towards common European cooperation, focusing upon resilience and the security of networks (European Commission, 2016).

While European digital sovereignty discourse was not explicitly tied to Toolbox plans at its inception, the update process was shaped by the broader 'geopoliticization' of EU trade policy over the 2017-2019 period and escalating strategic competition between the US and China (Meunier & Nicolaidis, 2019). During this period, the EU was encouraged to rethink its trade relationship with China and the US, which was already fraught after the Trump Administration's 'retreat' from multilateralism and its 'trade war' with China (ibid; Interviewee C; General Secretariat of the Council, 2020). For EU external action, 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).

Particularly, the Huawei debate was one episode which evinced the geopolitical dimension to critical digital infrastructure and European dependency on foreign suppliers

and tech ‘giants’ (Radu & Amon, 2021). In 2017, the US banned 5G technology supplied by Chinese state-backed telecommunications company Huawei on the charge of state-backed cyber espionage among other accusations (European Parliament, 2019). At the time, Huawei was leading in the European 5G market due to its cheap prices and purportedly high quality, rendering European telecommunications operators highly dependent on Chinese technology (ibid). Accordingly, the Huawei/5G security risks and ‘unhealthy’ foreign investment came to be understood as a significant hindrance to European digital sovereignty and technological autonomy (Friends of Industry, 2018). Thereafter, the relationship between finance and cybersecurity 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 (Interviewee B). In turn, the COVID-19 pandemic demonstrated how global interdependence, including digital value supply chains, could be weaponized (Interviewee E; European Commission, 2020c, 2020d). Consequently, the 5G Toolbox advanced a revised threat landscape and updated measures concentrated around strategic, technical and supporting actions for 5G technologies and foreign direct investment (NIS Cooperation Group, 2019). As the High Representative (HR/VP) Josep Borrell put it in 2020, ‘a foreign investment screening mechanism, reinforced trade instruments, a useful toolbox for 5G […] help with the construction of our political autonomy’ (European External Action Service, 2020). That same year, 5G network security was declared to be essential for ensuring Europe’s technological sovereignty (European Economic and Social Committee, 2020; European Commission, 2020e).

Collectively, examining the development of the 5G Toolbox evinces *comprehensive change* towards sovereignty, as both policy and discourse were significantly linked and oriented towards sovereigntist goals. Both European digital/technological sovereignty and strategic autonomy pervaded digital industrial policy (including 5G discussions) as relevant

and applicable concepts (see for example European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2019; European Commission, 2020a, 2020c; NIS Cooperation Group 2019). Given that both sovereigntist discourse *and* strategic autonomy have been referenced as key goals in cyber-relevant industrial policy, it is difficult to discern their individual influence(s) on policy change, which leads to their characterization as *indistinctive change.*

Coincident with latter updates to the EU's external CCB framework, the trajectory of Toolbox process overlaps with the von der Leyen Commission entry into office, when the discourse reached primacy in EU external action policy. As one interviewee stressed, at that point, the 5G update and industrial policies had acquired a 'self-conscious framing' around strategic autonomy as this was the Commission's 'selling point' (Interviewee K). However, the relationship between discourse and policy change was also shaped by changed geopolitical perceptions associated with 5G infrastructure and its implications for US and Chinese trade relationships (as detailed above); a shift in the Commission's focus to identifying which sectors had critical dependencies (such as 5G); and the Union's concerns about cyber resilience, which notably predated sovereignty discourse (Interviewees J, K; European Commission & High Representative of the Union for Foreign Affairs and Security, 2017; Juncos, 2017).

Summary

Overall, while 'European digital sovereignty' discourse has populated contemporary EU policy debates about EU external action, its influence on concrete policy changes in this domain has been uneven. Characterizing the relationship between discursive and policy change in yields two examples of *inconspicuous change*, with one policy area exemplifying *comprehensive change*. For all three cases, the main competing concepts in European sovereigntist discourse (European digital sovereignty and strategic autonomy) were used

interchangeably at the same frequency in policy discourse, rendering their specific role as concepts *indistinctive*.

Interestingly, the two cases of *inconspicuous* change vis-à-vis European digital sovereignty discourse have evinced practices of partial repackaging, whereby sovereignty has operated as a frame through which policymakers justify and/or legitimize their policy decisions *ex post* (Walker, 2008). For one, the European Parliamentary Research Service asserted *ex post* that the Cyber Diplomacy Toolbox is critical for making the EU 'strategically autonomous' and 'technologically sovereign' (Latici, 2020). Additionally, the EEAS credited the Cyber Diplomacy Toolbox as part of the EU's practical approach to 'enhance the EU's strategic autonomy' as part of the Union's *Strategic Compass* (European External Action Service, 2021). However, the official document for the *Compass* made no explicit references to the Toolbox in its discussion of how 'technological sovereignty' would be promoted (General Secretariat of the Council, 2022b). Secondly, the nascent Digital4Development Hub (which currently covers EU external CCB) highlighted how the 5G Toolbox would serve as the pathway for putting European digital sovereignty into practice with partners (European Commission, n.d-b). At the time of writing, the Digital4Development Hub continues to rely upon a 2017 *Staff Working Document* on 'mainstreaming digitalisation into development cooperation' penned by the European Commission (2017a), in which sovereignty discourse is notably absent.

Discussion

Below, the paper situates its findings in the broader context of EU external action policy change, attempting to shed further light about the evolution of European digital sovereignty discourse in EU external action policy. The goal of this discussion is to explore plausible drivers which could be tested by future research, not to evaluate the transferability of these mechanisms or their general validity. To that end, it considers several plausible

factors which could have shaped the relationship between discourse and changes to the Cyber Diplomacy Toolbox, EU external CCB programmes, and the 5G Toolbox.

Foremost, the paper documented how significant events in the global digital and cyber domains over the 2016-2020 period were influential for its three cases of *policy change* towards digital sovereignty. This coheres with extant scholarship, which has demonstrated how global events over this period—including rising global strategic competition, weaponized interdependence, and the decline of multilateralism—have partially shaped the EU's 'geopolitical Commission' (Haroche, 2022) and the geopoliticization of EU foreign policy, including in the areas of trade (Meunier & Nicolaidis, 2019) and the EU's partnerships with third countries (Cadier, 2019). However, as one official stressed to me, concerns about geopolitics, dependency and/or security risks do not necessarily beget European digital sovereignty *discourse* in the policy change process (Interviewee M). For the cases examined here, the 5G Toolbox update was the only case whereby European digital sovereignty discourse became entwined with risk perceptions of techno-geopolitical competition and global supply chain dependency issues. By contrast, while concerns around geopolitics, digital control, and cross-border risks were also influential in shaping the development of the Cyber Diplomacy Toolbox and external CCB projects, European sovereignty discourse was not seen as relevant and applicable to their development. Accordingly, the changed global geopolitical environment alone cannot sufficiently explain why European digital sovereignty discourse was linked to the 5G Toolbox *ex ante* but not the other two cases of change.

Additionally, it is plausible that three endogenous factors have also mediated this phenomenon: the division of competences, legitimacy concerns, and the ambitions of the von der Leyen Commission. First, Brussels' divergent competences over different areas of EU external action appeared to have influenced the uneven applicability and relevance of

the discourse to the paper's three cases of policy change. The institutional context shapes discursive interactions through structuring who speaks, where, and when, and over their decision-making capacity (Schmidt, 2011). Notably, since the EU's inception as a coal and steel community, industrial and economic policy have been considered *European* issues, thus endowing the Union's supranational authority over trade with a high degree of legitimacy (Haroche, 2022; Lutz & Karstens, 2021). Therefore, Brussels' historically greater decision-making role over trade compared to development cooperation policy and the CFSP could have provided a stronger baseline for advancing a *European* approach to digital sovereignty. Indeed, historical precedent is cited by Commission President von der Leyen in her announcement of the EU's current *Digital Strategy*: 'We successfully shaped other industries […] and we will now apply the same logic and standards in the new data-agile economy. I sum up all of what I have set out with the term "tech sovereignty"'(2020e). Her predecessor, Jean-Claude Juncker, articulated a similar logic in his *State of the Union* speech by asserting that 'the Euro must become the face and the instrument of a new, more sovereign Europe' as opposed to hard militarization (quoted in European Commission, 2018b).

Indeed, EU competences and legitimacy concerns could partially explain the discourse's absence in the development of the Cyber Diplomacy Toolbox, whereby reference to 'European sovereignty' was not applicable or relevant in a discussion that Member States believed pertained to their national *sovereignties* (Interviewee K, 2022). Despite recent efforts by the Commission to further encroach into matters of security and defence (Haroche, 2022), supranational competences remain heavily curtailed in the EU's CFSP, whereby decisions are made in the Council and authority over 'hard' security capabilities is firmly retained by Member States. Here, it should be noted that 'strategic autonomy' is generally a more comfortable concept in (European) military and security discourses compared to 'European sovereignty' (Interviewee R), and the concept of 'European strategic autonomy'

first emerged in the 2013 *Council Conclusions* on the EU's CDSP (General Secretariat of the Council, 2013). Nonetheless, 'strategic autonomy' was explicitly in reference to strengthening the EU's technological and defence *industry.* This only reinforces the pattern identified by this study: that European digital sovereignty discourse has remained most relevant and applicable to (cyber) industrial policy in comparison to other areas of foreign and security policy.

Compared to the CFSP, EU supranational institutions also enjoy greater influence over development cooperation projects (Prontera & Quitzow, 2022), such as external CCB, through shared competences with Member States. Yet, despite Brussels' relatively high institutional influence over the development policymaking process compared to the CFSP, interviewee responses suggest a legitimacy problem: that advancing European digital sovereignty concepts were seen as *less appropriate* in cooperative settings with partners. Multiple EU officials independently voiced worries that European digital sovereignty could be 'misunderstood' as a guise for imperialism, colonialism, and/or 'traditional' geopolitics (Interviewees A, B, C, F, E, T). Interviewees were at pains to clarify that the EU's CCB projects in Africa were *not* carried out in a geopolitical way (Interviewees A,E), and that European sovereignty was not a foreign 'diktat', but 'already an explanation [for] how we understand this…international aspect,' (Interviewee A). Thus, officials argued that EU external CCB projects are not designed to compete with China's *Belt and Road Initiative* (BRI), but rather to 'empower partners' (Interviewees A,T), although recent EU development finance projects have been explicitly designed in response to the BRI (Haroche, 2022).

More broadly, reputational concerns about what European digital sovereignty *means* seem to be particularly aggravated in multilateral settings: officials have been concerned with how 'European digital sovereignty' has communicated the EU's global position vis-à-

vis its partners, particularly the US (Interviewee C). As one EEAS official stated, '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). This official expressed their dismay 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' (ibid). Other interviewees from the EU Commission and the UK civil service respectively conveyed their exasperation about uncovering the meaning of these terms and explaining them to third countries (Interviewees E,F). 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). Thus, the cooperative nature of EU external CCB projects could reinforce officials' reluctance to invoke European sovereignty discourse, given the risks of its misinterpretation for attracting and maintaining partnerships with third countries. Collectively, these responses suggest that 'European sovereignty' may come into tension with the EU's historical self-representation as a global actor and diplomatic partner, which is premised upon an eschewal of traditional geopolitics and colonialism (Fisher Onar & Nicolaïdis, 2013; Guzzini, 2012). Nonetheless, this hesitancy is not shared by all divisions of the EU; for some, the concept was seen as necessary to have 'conversations with the big geopolitical powers' including in 5G discussions and the realization that Member States cannot act alone to secure their strategic interests (Interviewee A, see also Haroche, 2022).

Further to this point, interviews revealed significant conceptual disagreement over the meaning(s) of European digital sovereignty/strategic autonomy across EU policy communities. On the one hand, different EU policy communities have conflated strategic autonomy and European sovereignty as means/ends over time (Timmers, 2018, 2022;

European Commission 2020e; cf. General Secretariat of the Council, 2020, p. 4; Madiega, 2020). On the other, different Member States have preferred ‘strategic autonomy’ as an alternative concept to ‘European digital sovereignty’ and vice versa (Interviewees B,C). Consequently, the Council of the EU has been divided in terms of what ‘European sovereignty’ means to the EU’s global positioning and ambitions: whereas some Member States understand it as a move towards protectionism and others have rejected this ‘fortress Europe’ conception and emphasized the importance of openness for European sovereignty (Interviewees A,B,D). More broadly, a recent survey of European policymakers highlighted that Member States disagree on the level of ambition for ‘European strategic autonomy’ and on which policy areas should be prioritized to meet this objective (Franke & Varma, 2019; pp. 12, 20). Such internal contestation has important implications for vertical and horizontal policy coordination (see also Haroche, 2022). Fuzziness and disagreement on key concepts can stymie policy coordination, especially in consensus-based bodies that are vulnerable to Member State vetoes (e.g. the CFSP), as opposed to areas of concentrated EU authority (e.g. trade). Contestation may therefore lead to the discourse’s omission in the policymaking process (as it degrades coordination) or in the final publication and framing of policy documents. Indeed, as demonstrated by interviewee remarks on the Cyber Diplomacy Toolbox process, contestation could partially explain why European digital sovereignty was not relevant or applicable to CFSP policy changes (Interviewee K), when the opposite was observable in the development of the 5G Toolbox.

Exploring how these potential drivers interrelate suggests important interactive effects relevant to the relationship between digital sovereignty discourse and the cases examined. Particularly, the finding that European digital sovereignty discourse shaped the 5G Toolbox process but failed to drive the Cyber Diplomacy Toolbox and external CCB initiatives substantiates Adler-Nissen and Gammeltoft-Hansen’s (2008) argument about

'sovereignty frames.' Sovereignty frames, they contend, are expressed to reinforce and legitimize *existing* authoritative capacities in cases of a perceived loss of control. Accordingly, this argument is premised upon the influence of legitimate authority, competences, *and* perceptions of exogenous events. The 5G Toolbox update illustrates this dynamic; it was developed in response to the Union's concerns about its diminishing role as an economic security provider and technological leader vis-à-vis other global actors (Friends of Industry, 2018). Further, as Radu and Amon (2021) observed, the Union lacks competence in national security, and therefore resorted to a 'market-based policy toolbox built on risk assessment' for its Member States to use at the national level. Elsewhere, Calderaro and Blumfelde's analysis of the EU's approach to AI found that Brussels has 'traditionally adopted a regulatory approach to protect its digital market', and European digital sovereignty 'has been mostly tied to the idea of the EU as a regulatory actor' in the global context (2022, pp. 417-18).

Furthermore, the cases of the Cyber Diplomacy Toolbox and external CCB projects evince how certain policy coordination and cooperation dynamics (e.g. consensus-based and diplomatic contexts) can interact with discursive contestation to constrain a discourse's effect on policy change (Franke & Varma, 2019). Lastly, the paper explored how reputational concerns about expressing 'European digital sovereignty' in multilateral contexts (e.g. external CCB) has generated hesitancy about using the discourse as a justification in diplomatic contexts. This suggests that the discourse has significant implications for the EU's identity and its perceptions of legitimacy vis-à-vis external partners (Csernatoni, 2022; Barrinha & Christou, 2022). Ultimately, the popularization of European digital sovereignty discourse in EU policy —despite enduring vertical and horizontal contestation about its meaning—underscores the discourse's broader importance for the Union's contemporary approach to global affairs.

Conclusion

During the years of the discourse's mainstreaming into EU external action (2017-2022), cyber instruments have served as important enablers for operationalizing Brussels' control over the digital domain (Barrinha & Christou, 2022; Bellanova et al., 2022). However, throughout this period, European digital sovereignty discourse has enjoyed a varied relationship to three policy changes towards sovereignty in EU external action: the Cyber Diplomacy Toolbox, EU external CCB projects, and the 5G Toolbox. Whereas the discourse *comprehensively* shaped changes to the 5G Toolbox, its relationship to the other two cases of policy change were *inconspicuous*. Additionally, the paper explored how the interaction of exogenous and endogenous factors to EU external action policy plausibly shaped this relationship, including transformative experiences of events, EU competences/legitimacy constraints, discursive contestation, and coordination/cooperation dynamics. These findings contribute to burgeoning scholarship on European digital sovereignty discourse in the context of EU foreign policymaking and EU cybersecurity literature.

By exploring the potential drivers relevant to the paper's empirical findings, the study also highlighted the complex, evolving nature of European digital sovereignty discourse and EU policymaking. As 'strategic autonomy is […] a process of political survival' for the Union (Borrell, 2020), the relationship between European digital sovereignty discourse and policy change remains an open question for future scholarship. At the time of writing, the European digital sovereignty constitutes a priority for the current French Presidency of the Council and the von der Leyen Commission (EU Cyber Direct, 2022). To this end, Brussels has announced its intentions to push through concrete policies relevant to digital sovereignty on AI, supercomputing, and in line with the Strategic

Compass (ibid; Calderaro & Blumfelde, 2022). Notably, through the recently formed US-Trade Technology Council, Brussels and Washington have produced a common outlook on '6G' (White House, 2023). These initiatives provide ripe opportunities for future scholarship concerned with the EU's digital sovereignty ambitions. Therefore, the paper's discussion of potential drivers offers a fruitful point of departure for examining the relationship between European digital sovereignty discourse and EU external action policy change.

Chapter 5 References

Adler-Nissen, R., & Gammeltoft-Hansen, T. (Eds.) (2008). *Sovereignty Games: Instrumentalizing State Sovereignty in Europe and Beyond*. Palgrave MacMillan.

Bacchi, C.L, & Goodwin, S. (2016). *Poststructural Policy Analysis: A Guide to Practice*. Palgrave MacMillan.

Barkawi, T. (2016). Decolonising War. *European Journal of International Security* 1(2): 199–214.

Bartolini, S. (2006). *Restructuring Europe: Centre Formation, System Building, and Political Structuring between the Nation State and the European Union*. Oxford Scholarship Online.

Barrinha, A., & Christou, G. (2022). Speaking Sovereignty: The EU in the Cyber Domain. *European Security 31*(3), 356-376.

Beach, D. & Pedersen, R.B. (2019). *Process-Tracing Methods: Foundations and Guidelines*. University of Michigan Press.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/Sovereignty and European Security Integration: An Introduction. *European Security 31*(3), 337-355.

Bendiek, A, Ålander, M., and Bochtler, P. CFSP: The capability-expectation gap revisited: a
data-based analysis. doi:10.18449/2020C58.

Bialasiewicz, L. (2015). *Europe in the World: EU Geopolitics and the Making of European Space.* Routledge.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World.* Columbia Law School.

Broeders, D., Csernatoni, R., Irion, K., Kaminska, M., Monti, G., Robles-Carrillo, M., Soare, S. R., & Timmers, P. (2022). Digital Sovereignty: From Narrative To Policy? *EU Cyber Direct.* https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy.

Buzan, B., & Wæver, O. (2003). *Regions and Powers: The Structure of International Security*. Cambridge University Press.

Cadier, D. (2019). The Geopoliticisation of the EU's Eastern Partnership. *Geopolitics,* 24(1), 71-99. https://doi.org/10.1080/14650045.2018.1477754.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security 31*(3), 415-434.

Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies* 55 (6): 1254–72.

Carrapico, H., & Farrand, B. (2020). Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy. *Journal of European Integration 42*(8), 1111–26.

Chander, A., & Sun, H. (2021). Sovereignty 2.0. *Georgetown Law Faculty Publications and Other Works* 2404.

Christou, G. (2019). The Collective Securitisation of Cyberspace in the European Union. *West European Politics* 42(2), 278–301.

Clarke, A.E., Friese, C., & Washburn, R. (2015). *Situational Analysis in Practice: Mapping Research with Grounded Theory.* Routledge, Taylor and Francis.

Collett, R. (2021). Understanding cybersecurity capacity building and its relationship to norms and confidence building measures, *Journal of Cyber Policy*, 6(3), 298-317.

Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States (2019) [Regulation no. ST/7299/2019/INIT].

Council of the European Union. (2016). *Six Monthly Report on the Implementation of the Cyber Defence Policy Framework* [9701/16]. Accessed from https://www.statewatch.org/media/documents/news/2016/jul/eu-council-cyber-defence-implementation-report-9701-16.pdf.

———. (2017, June 19). *Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox.

———. (2021a). *A digital future for Europe.* https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/.

———. (2021b, February 3). *Digital sovereignty is central to European strategic autonomy - Speech by President Charles Michel at "Masters of digital 2021" online event* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/.

———. (2022, March 21). *A Strategic Compass for a stronger EU security and defence in the next decade* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/.

———. (2023, June 26). *Digital diplomacy: Council sets out priority actions for stronger EU action in global digital affairs [press release].* https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/digital-diplomacy-council-sets-out-priority-actions-for-stronger-eu-action-in-global-digital-affairs/

Council of the European Union Presidency (2016). *Cyber capacity building: towards a strategic European approach* [8732/1/16]. https://www.statewatch.org/media/documents/news/2016/jul/eu-council-cyber-capacity-building-8732-1-16.pdf.

Coyne, H. (2019). The Untold Story of Edward Snowden's Impact on the GDPR. *The Cyber Defense Review*. https://www.jstor.org/stable/26843886

Cremona, M., & Scott, J. (Eds). (2019). *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*. Oxford University Press.

Csernatoni, R. (2022). The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty. *European Security 31*(3), 395–414.

Ebbinghaus, B. (2005). When Less is More: Selection Problems in Large- N and Small- N Cross-National Comparisons. *International Sociology 20*(2): 133-152.

EU Cyber Direct. (2022, January 12). *Digital Regulation and Tech Sovereignty among the Priorities of the French Presidency* [Press release]. https://eucyberdirect.eu/news/digital-regulation-and-tech-sovereignty-among-the-priorities-of-the-french-presidency.

Eudaily, S.P. & Smith, S. Sovereign Geopolitics? Uncovering the 'Sovereignty Paradox. *Geopolitics 13*(2): 309–34.

European Commission. (2010). *A Digital Agenda for Europe* [COM(2010)245 final].

———. (2016). *5G for Europe: An Action Plan* [COM/2016/0588 final].

———. (2017a). *Digital4Development: Mainstreaming Digital Technologies and Services into EU Development Policy* [Working paper, SWD(2017) 157 final].

———. (2017b). *Reflection paper on the future of European defence* [COM(2017) 315].

_____/ (2017c). *President Jean-Claude Juncker's State of the Union Address 2017* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165.

———. (2018a). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Neighbourhood, Development and International Cooperation Instrument* [COM/2018/460 final].

———. (2018b, September 12.) *President Jean-Claude Juncker's State of the Union Address 2018* [Press release]. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en_0.pdf.

———. (2020a). *A New Industrial Strategy for Europe* [COM(2020) 102 final].

———. (2020b). *Shaping Europe's Digital Future*. https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-

digital-future-feb2020_en_4.pdf.

———. (2020c). *Strategic Foresight Report*, [COM/2020/493 final].

———. (2020d). *Communication on the Action Plan on Synergies and Cross-Fertilisation between Policies and Instruments Relevant to the Civil, Defence and Space Industries* [Document Ares(2020)5040558].

———. (2020e, February 19). *Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/AC_20_260.

———. (2021a, March 9). *Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030* [press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983

———. (2021b, June 15). *EU-US launch Trade and Technology Council to lead values-based global digital transformation* [press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2990

———. (2021c, December 1). *Global Gateway: Up to €300 Billion for the European Union's Strategy to Boost Sustainable Links around the World* [press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6433.

———. (2022a). *EU-Africa: Global Gateway Investment Package*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en

———. (2022b). *Roadmap on critical technologies for security and defence.* [COM(2022) 61final]. https://commission.europa.eu/system/files/2022-02/com_2022_61_1_en_act_roadmap_security_and_defence.pdf

———. (2022c, February 2). *New Approach to Enable Global Leadership of EU Standards*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661.

———. (2022d, June 2). *Cybersecurity in the DIGITAL Europe programme* [press release]. https://digital-strategy.ec.europa.eu/en/activities/cybersecurity-digital-programme

———. (2022e, June 7). *5G Action Plan* [webpage]. https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan

———. (Last updated August 23, 2023). *Cybersecurity in the DIGITAL Europe programme* [webpage]. https://digital-strategy.ec.europa.eu/en/activities/cybersecurity-digital-programme.

———. (n.d.-a) *A future-proof security environment* [webpage]. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union/future-proof-security-

environment_en

———. (n.d.-b) *Responsible digitalisation* [webpage]. https://international-partnerships.ec.europa.eu/policies/digital-and-infrastructure/responsible-digitalisation_en.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. 2016. *Joint Framework on Countering Hybrid Threats: A European Union Response* [JOIN/2016/018 final].

———. (2017). *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU* [JOIN(2017) 450 Final].

———. (2019). *EU-China—A Strategic Outlook* [JOIN(2019) 5 final].

———. (2020). *The EU's Cybersecurity Strategy for the Digital Decade* [JOIN/2020/18 final].

———. (2021). *Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade* [JOIN/2021/14 final].

European Economic and Social Committee. (2020, September 8). *Secure 5G Deployment-EU Toolbox* [Opinion paper, TEN/704].

European External Action Service. (2020, September 14). Cyber Diplomacy and Shifting Geopolitical Landscapes
[Press release]. https://www.eeas.europa.eu/eeas/cyber-diplomacy-and-shifting-geopolitical-landscapes_en.

European External Action Service. (2016). Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy [EUGS]. https://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

European Parliament. (2019). *Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them* [P8_TA(2019)0156].

European Union Committee. (2010). *Protecting Europe against Large-Scale Cyber-Attacks*. United Kingdom House of Lords Publications (Report). https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6802.htm

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2023). Digital sovereignty – rhetoric and reality: special issue framework paper. *Journal of European Public Policy*. Forthcoming.

Fisher Onar, N., & Nicolaïdis, K. (2013). The Decentring Agenda: Europe as a Post-Colonial Power. *Cooperation and Conflict 48* (2), 283–303.

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization 52* (4), 887–917.

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology 33*, (3): 369–78. https://doi.org/10.1007/s13347-020-00423-6.

Franke, U. & Varma, T. (2019). Independence play: Europe's pursuit of strategic autonomy. *European Council on Foreign Relations.* https://ecfr.eu/wp-content/uploads/Independence-play-Europes-pursuit-of-strategic-autonomy.pdf.

Friends of Industry (2018, December 18). *6th Ministerial Meeting joint statement*. https://www.bmwk.de/Redaktion/DE/Downloads/F/friends-of-industry-6th-ministerial-meeting-declaration.pdf?__blob=publicationFile&v=6

General Secretariat of the Council. (2013). *Conclusions* [EUCO 217/13].

———. (2015). *Council Conclusions on Cyber Diplomacy* [6122/15]. Council of the European Union.

———. (2016). *Council Conclusions: Mainstreaming Digital Solutions and Technologies in EU Development Policy* [6122/15]. Council of the European Union.

———. (2017). *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* [10474/17]. Council of the European Union.

———. (2018). *EU External Cyber Capacity Building Guidelines - Council Conclusions (26 June 2018)* [10496/18]. Council of the European Union.

———. (2019). *Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States*.

———. (2020a). *Shaping Europe's Digital Future - Council Conclusions* [2020/C 202 I/01]. Official Journal of the European Union.

———. (2022a). *Council Conclusions on EU Digital Diplomacy* [11406/22]. Council of the European Union.

———. (2022b). *A Strategic Compass for Security and Defence* [7371/22]. Council of the European Union.

Guzzini, S. (2012). *The Return of Geopolitics in Europe?: Social Mechanisms and Foreign Policy Identity Crises.* Cambridge University Press.

Haroche, P. (2022). A 'Geopolitical Commission': Supranationalism Meets Global Power Competition. *JCMS: Journal of Common Market Studies*, 61: 970–987.

Hill, C. (1993), The Capability-Expectations Gap, or Conceptualizing Europe's International Role, *Journal of Common Market Studies*, 31: 305–328.

Juncos, A.E. (2017). Resilience as the New EU Foreign Policy Paradigm: A Pragmatist

Turn? *European Security* 26 (1): 1–18.

Kuner, C. (2019). The Internet and the Global Reach of EU Law. In Cremona, M. & Scott, J., (Eds.) *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, edited by
Oxford University Press.

Latici, T. (2020). *Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence* (Report no. PE 651.937). European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf

Laurer, M., & Seidl, T. (2021). Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation. *Policy and Internet 13*(2), 257–77.

Lipscy, P. (2020). COVID-19 and the Politics of Crisis. *International Organization, 74*(S1), E98-E127.

Lutz, P., & Karstens, F. (2021). External Borders and Internal Freedoms: How the Refugee Crisis Shaped the Bordering Preferences of European Citizens. *Journal of European Public Policy 28* (3), 370-388.

Madiega, T. (2020). *Digital Sovereignty for Europe Digital Sovereignty: State of Play* (Report no. PE 651.992). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

Manners, Ian. (2002). Normative Power Europe: A Contradiction in Terms? *Journal of Common Market Studies 40*(2), 235-58.

Moerel, L., and Timmers, P.,2021.*Reflections on digital sovereignty*. Rochester, NY: Social Science Research Network.

Monsees, L., & Lambach, D. (2022). Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity. *European Security 31(*3), 377–94.

Moravcsik, A. (1998). *The choice for Europe. Social purpose and state power from Messina to Maastricht.* Routledge.

NIS Cooperation Group. (2019). *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks* (Report). European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

Pawlak, P. (2017). *Building Capacities for Cyber Defence*. (Report). European Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert%2026%20Cyber%20development.pdf.

———. (2018). *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building* (Report: ISBN 978-92-9198-756-6). EUISS Task Force for Cyber

Capacity Building, European Commission. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf.

Pawlak, P., & Barmpaliou, P-N. (2017). Politics of cybersecurity capacity building: conundrum and opportunity. *Journal of Cyber Policy 2* (1): 123-144.

———. (2023). *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building: Second Edition.* Tallinn: European Union. https://www.eucybernet.eu/wp-content/uploads/2023/11/operational-guidance-for-the-eu-international-cooperation-on-ccb-1-1.pdf.

Prontera, A., and Quitzow, R. (2023) Catalytic Power Europe: Blended Finance in European External Action. *JCMS: Journal of Common Market Studies*, 61: 988-1006. https://doi.org/10.1111/jcms.13442.

Radu, R. & Amon, C. (2021). The governance of 5G infrastructure: between path dependency and risk-based approaches. *Journal of Cybersecurity* 7(1), 1-16.

Reding, V. (2016). *Digital Sovereignty: Europe at a Crossroads.* EIB Institute. https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf.

Renard, T. (2018). EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain. *European Politics and Society 19(*3), 321–37.

Schmidt, V. (2002). *The Futures of European Capitalism*. Oxford University Press.

———. (2011) Speaking of Change: Why Discourse Is Key to the Dynamics of Policy Transformation. *Critical Policy Studies* 5(2): 106–26.

Schmidt V. & Radaelli, C.M. (2004). Policy Change and Discourse in Europe: Conceptual and Methodological Issues. *West European Politics 27*: 183-210.

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive Design: Concepts and Processes.* Routledge, Taylor & Francis.

Sjursen, H. (2011). Not so intergovernmental after all? On democracy and integration in European Foreign and Security Policy. *Journal of European Public Policy 18(*8), 1078–95.

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

Thomson, J. (1995). State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research. *International Studies Quarterly 39*(2), 213-233.

Timmers, P. (2018). The European Union's Cybersecurity Industrial Policy. *Journal of Cyber Policy* 3(3), 363–84.

———. (2022, February 24). Digital Sovereignty, the Netherlands, the EU: Some Elements (Paper presentation). University of Warwick, United Kingdom.

Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri D., & Dufkova, A. (2017). *Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU* (Report no. PE 603.175). European Parliamentary Research Service.

Walker, N. (2008). The Variety of Sovereignty. In Adler-Nissen, R., & Gammeltoft-Hansen, T (Eds.). *Sovereignty Games: Instrumentalizing State Sovereignty in Europe and Beyond* (pp. 21-32). Palgrave MacMillan.

White House. (2023, May 31). *U.S.-EU Joint Statement of the Trade and Technology Council* [press release]. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/

Wong, R., & Hill, C. (2011). *National and European Polices Towards Europeanization.* Routledge.

Zanders, J-P. (2009, March 10). *Cyber Security: What Role for CFSP?* (Report no. IESUE/SEM(09)04). General Secretariat of the Council of the European Union, European Union Institute for Security Studies. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_cyber_security_1_.pdf

Appendix - List of Interviews

Interviewee code	Date	Organization/Institution	Seniority
A	05/03/21	EEAS, Lead cyber engagement and national representative	High
B	11/03/21	Permanent Representation of Estonia to the EU	Medium
C	12/03/21	European Council on Foreign Relations	Senior
D	18/03/21	EEAS	High
E	25/03/21	European Commission – Executive cabinet	Medium
F	16/03/21	European Union Institute for Security Studies (Cyber Capacity Building Task Force)	Medium
G	9/09/22	(Former) Member State – United Kingdom, national government	High
H	15/09/22	European Union Institute for Security Studies, Cyber Policy	High
I	25/04/22	EEAS, Cyber Policy	High
J	30/05/22	European Commission, DG INTPA	Low
K	02/08/22	European College of Commissioners	High
M	06/05/22	European Commission, DG CNECT	Medium
N	17/05/22	European Commission, CC TT	High
O	31/05/22	Council of Europe	High
P	11/05/22	European Commission	High
Q	20/04/22	European Commission, DG NEAR	Low
R	05/05/22	European Commission, DG CNECT	Senior
S	16/05/22	EEAS, Eastern Partnership	Low
T	25/04/22	EEAS, Global Gateway	Senior

Article Acknowledgments

I am very grateful to the interviewees for their time and their generous support of my research, and to the three anonymous referees for their invaluable feedback and patience. Further, I would like to thank the Co-Editors of this Special Issue, Gerda Falkner, Sebastian Heidebrecht, Anke Obendiek and Timo Seidl, whose continued support greatly improved the paper. Drafts of this article were presented at the University of Vienna's workshop (2021) and later as part of a panel at the 11th annual conference of the ECPR Standing Group on the EU in summer 2022, and I appreciate the feedback and insights from the participants in these fora. Finally, I would like to gratefully acknowledge Nuffield College and the Economic and Research Council for funding my research [ES/P000649/1].

Data availability statement:

The author obtained approval for conducting research with human participants from the DPIR Departmental Research Ethics Committee (DREC) in accordance with the procedures laid down by the University of Oxford for ethical approval of all research involving human participants, and informed consent from all interviewees. Ethics approval reference numbers are SSH_DPIR_C1A_21_005 and SSH_DPIR_C1A_22_008. For interview dates, refer to the appendix. Due to the politically sensitive nature of the research and in line with interviewee consent, interview data cannot be made openly available. However, the archival sources used by the study are openly available, accessible at the EURLEX database and as noted in the reference section of the paper.

Funding and mandatory open access statement:

This work was supported by the Economic and Research Council [ES/P000649/1] and Nuffield College.

Chapter 6: Creating a ‘European’ cyberspace: How spatial (b)ordering and ontological security drives have underpinned the EU’s evolution as a global actor

Abstract

The last decade has seen the global rise of territorialising moves in and through cyberspace. However, extant international relations scholarship has tended to privilege the material and structural drivers of actors’ geostrategic behaviour, thereby struggling to explain the European Union’s recent embrace of these ambitions in its global approach to cyberspace. To address these theoretical and empirical gaps, this paper asks: how has the EU’s engagement with spatial (b)ordering practices in cyberspace shaped its evolution as a strategic cyber actor, and to what extent have ontological security drives underpinned this relationship? Diverging from dominant accounts, this paper develops a novel theoretical framework which foregrounds the relationship between spatial (b)ordering moves, ontological security, and geostrategic behaviour. Drawing upon documentary evidence and over two dozen elite interviews, my discourse analysis reveals how, over the 2009-2024 period, EU actors have deployed various spatial (b)ordering moves to manage the Union’s ontological security needs in a constantly evolving global environment. The paper’s critical ontological approach foregrounds the co-constitutive relationship between the environmental features of cyberspace and global actors’ ontological security in and through cyberspace. Ultimately, by bridging theoretical and empirical gaps between ontological security and critical geopolitics scholarship in IR, this paper contributes to an emerging IR research agenda on the spatio-temporal liminality of ‘cyberspace’ and its relationship to the EU’s development as a foreign policy actor.

Keywords: *Critical geopolitics, cyberspace, ontological security, European Union, digital interdependence*

‘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)

Introduction

In 2020, on the heels of a highly digitalized year, the European Commission and the European External Action Service jointly declared the European Union’s desire to ‘learn the language of geopolitical power’ (Borrell, in Weiler, 2020) and to achieve ‘European digital sovereignty’ (von der Leyen, 2019). Brussels’ geostrategic turn has taken place against the background of escalating geopolitical competition and weaponized interdependence fears in cyberspace (Kello, 2022), which have widely evoked sovereigntist impulses in Europe, Africa, and Asia (Carver, 2024a). Under this new geostrategic agenda, the EU’s global role in cyberspace has become a linchpin of its external action in a ‘world of moving geopolitical plates’ (European External Action Service, 2020).

Despite this wider context, extant international relations (IR) literature has been puzzled by the EU’s geostrategic transformation. Brussels is widely considered to be ill-disposed for geostrategies, given the Union’s complex relationship to territoriality, its post-Westphalian stance, and its stunted coercive capabilities. Besides, adopting geostrategies in cyberspace is complicated by the domain’s structural makeup, which deviates from ‘Westphalian territoriality’ and state sovereignty (Betz & Stevens, 2013; Balzacq & Dunn Cavelty, 2016).

The EU’s puzzling geostrategic turn exposes two broader gaps in IR scholarship regarding the emergence and drivers of geostrategic behaviour in and through cyberspace. First, while scholars have scrutinized states’ sovereigntist and geopolitical approaches towards cyberspace (see for example Pohle & Voelsen, 2021; Glasze et al., 2022; Chander & Sun, 2021; Buchanan, 2020), these debates have often elided more critical questions about spatial (b)ordering—that is, the ideas, practices, and technologies producing and demarcating space (Lambach, 2020). Second, and relatedly, we know very little about the

ontological security foundations of geostrategic behaviour in cyberspace, particularly how these dynamics have been constituted by various spatial (b)ordering moves. Distinct from material security concerns, ontological security is an actor's quest to maintain a stable 'sense of Self' and 'trust that the world is what it appears to be' (Kinnvall 2004, p. 746). Elsewhere, scholars have demonstrated that spatial (b)orders are both exercises of (material) power and representational practices which seek to 'emplace' an actor's conception of their self and the world (see for example Lambach, 2024; Branch, 2024).

By foregrounding these dynamics, we can improve our understanding about the characteristics and drivers of geostrategic behaviour in and through cyberspace, including in the case of the EU. While IR scholarship has equivocated that cyber insecurities are ontologically disruptive for actors, the relationship between geopolitical behaviour and ontological insecurities in this context has been undertheorized. Furthermore, scholars have characterized the EU as an 'anxious community' (Mitzen, 2018a) battling with a 'decades-long existential crisis' (Tocci, 2021), thereby implying that such concerns may shape the EU's strategic behaviour in and through cyberspace.

To redress these critical gaps, this paper asks: How has the EU's engagement with spatial (b)ordering practices in cyberspace shaped its evolution as a (geo)strategic cyber actor, and to what extent have ontological security drives underpinned this relationship? More broadly, what are the implications of this theoretical approach for our understanding of strategic behaviour in cyberspace?

To answer these questions, this paper makes two analytical moves. First, the article theorizes that cyber insecurities may trigger actor's ontological security management behaviour in and through cyberspace. Second, this paper holds that this behaviour can manifest as spatial (b)ordering practices, including geopolitical and sovereigntist discourses. Specifically, I theorize that actors may engage *1) routinized spatial (b)ordering strategies;*

2) discourses of demarcation; and *3) productive spatial adaptations* to manage their ontological security in and through cyberspace. However, these strategies are not panaceas to an actor's ontological security struggles: efforts to better 'locate' the self through spatial (b)ordering and role adaptations may introduce further tensions, paradoxes, and insecurities in the actor's self-representation.

To explore the utility of this framework in the case of the EU, this paper examines key strategic developments to the EU's role as a global cyber actor over the 2009-2024 timeframe, anchoring the analysis in the 2013, 2017, and 2020 updates of the Union's cyber strategies and key strategic changes to the EU's external action approach. Throughout this period, I draw upon scores of relevant primary source documents and over two dozen elite interviews with EU policymakers to probe for evidence of spatial (b)ordering moves and ontological security management strategies.

My empirical findings support my theoretical framework by revealing how the EU's engagement with spatial (b)ordering moves is not only a reaction to systemic changes or material security concerns, but ontological security drives. Across the 2009-2024 period, I show how spatial bordering practices have been leveraged by EU actors as strategies to manage the Union's ontological security needs in a constantly evolving global environment. After establishing a 'European' cyberspace through the Union's first cyber strategy, the Union experienced a period of instability and ontological rupture during the 2014-2018 timeframe, whereby material 'cross-border' threats were not only framed as physical security issues, but inherent to the EU's existence as a global political actor. The increasingly insecure global context, as well as the convergence between cybersecurity and core areas of EU competences (e.g. economic security and trade) raised both physical and ontological security concerns for EU institutions, shaping the EU's explicit embrace of geostrategic logics from 2018-2024. This reveals how the EU's geostrategic role construction in

cyberspace has been an ontologically fraught, affective process, centered around managing ontological insecurities relevant to the EU's position in global cyberspace.

Accordingly, the contributions of this paper challenge dominant views about the EU's geostrategic turn in and through cyberspace (as advanced by structuralist and materialist perspectives) by emphasizing two understudied yet important facets to the EU's evolution as a global cyber actor: spatial (b)ordering moves and ontological security drives. In so doing, I contribute to scholarship on EU cyber policy incoherence and more longstanding work on the EU's evolving actorness in international relations (see for example Manners, 2002; Diez, 2010; Klose 2018, 2022). More broadly, by bringing sociopsychological theoretical tools into further dialogue with cyber-IR and EU Studies, I contribute to further theory development in cyber-IR about the relationship between geopolitical behaviour and sovereignty from a critical perspective, offering fresh analytical tools to understand the relationship between geostrategic competition and ontological security drives in the digital age.

The paper proceeds along the following lines. First, I review extant approaches to the EU's role as a cybersecurity actor, including the Union's recent geostrategic turn, together with wider IR scholarship on cyber-geopolitics. Next, I lay out my framework and methodological approach. Subsequently, I leverage this approach to make sense of the EU's development as a global cyber actor over the 2009-2024 period. Finally, I evaluate my empirical findings and draw conclusions about their implications for my research inquiries.

Material security, territoriality, and the EU's puzzling geostrategic behaviour in and through cyberspace

Extant scholarship on cyber-geopolitics has emphasized the complex territoriality of cyberspace as shaping actors' geostrategic behaviour. However, it has tended to rely upon

realist, state-centric assumptions, which have limited analytical purchase in explaining the EU's geostrategic turn. Elsewhere, critical scholarship has underscored the sociotechnical and co-constitutive nature of cyberspace, providing a valuable point of departure for theorizing how and why spatial (b)ordering moves and ontological security drives could shape actors' geostrategic behaviour. I review these two strands of literature below.

Early observers of the internet tended to treat cyberspace as separate from the whims of states and Westphalian territoriality, outright dismissing the possibility of geopolitical and sovereigntist claims (Barlow, 1996) or approaching the domain as deracinated from other spatial contexts (see also Liebetrau & Monsees, 2024, p. 1053; cf. Cohen, 2007; Betz & Stevens, 2013). This was partly due to the domain's complex territoriality and the significant role of the private sector and 'Big Tech' companies (Chander & Sun, 2021; Glasze et al., 2022). However, the 2010s saw an influx of geospatial analogies (Betz & Stevens, 2013), coinciding with academic and political recognition that geostrategic objectives could—and were—pursuable in and through cyberspace (Branch, 2024; Pohle & Voelsen, 2021).

Despite the rising popularity of geostrategic approaches to cyberspace, the EU has been considered inherently unsuitable for advancing explicit geopolitical and sovereigntist objectives in its external action approach. As Bauerle Danzman and Meunier observed, 'Neither its history nor its unique institutional structure suggested that the EU would be well positioned for this [geopolitical] turn,' (2023, p. 1097). Brussels' longstanding foreign policy identity and 'origin myth' as emerging from the ashes of traditional 'bloody geopolitics' (Fisher-Onar & Nicolaidis, 2015; Guzzini, 2012), together with its dynamics of 'shared' and 'pooled' sovereignty with Member States (Moravcsik, 1998; Bickerton et al., 2021) renders it ill-disposed to embrace 'the language of geopolitical power' and *European* sovereignty at the supranational level.

Indeed, for orthodox strategic studies debates on cyber-geopolitics, the EU's geostrategic approach to cyberspace constituted a highly surprising—if quixotic—turn. Such accounts have privileged state-centric, structuralist, and/or 'power politics' approaches (Liebetrau & Monsees, 2024), emphasizing the significance of cyberwarfare capabilities and a strong intelligence arm for exercising (cyber) power and competing geostrategically in and through cyberspace (Cai, 2018; Kello, 2017; Wu, 2017; see also Slayton, 2016). Given the EU's weak cyber capabilities, stunted competences in traditional security matters, and self-declared 'technological deficit' (Borrell, 2024), strategic studies literature had tended to position the EU as the geopolitical '*playground'* instead of a geopolitical *player* capable of advancing spatial (b)ordering moves (Weber, 2020; see for example Sliwinski, 2014).

With a similar emphasis on material variables, the EU Studies literature has largely cast Brussels' nascent geostrategic role in terms of its geoeconomic and regulatory influence (Herranz-Surralléz et al., 2023; Fahey, 2024; Drezner et al., 2021; Bradford, 2023; Heidebrecht, 2023). In such debates, the EU's changing material security concerns are widely credited as key drivers of this transformation (Herranz-Surrallés et al., 2024; Bauerle Danzman & Meunier, 2024; Carrapico & Farrand, 2024; Farrand et al., 2024; Haroche, 2023; Broeders et al., 2023). Such accounts have emphasized the causal influence of recent external shocks to the Union's physical security, paired with endogenous institutional constraints, as triggering the 'geopoliticization' of multiple EU policy areas, including external relations, (cyber)security, and trade (Herranz-Surralléz et al., 2023, p. 923; see for example Carrapico & Farrand, 2024).

Nonetheless, such 'geopoliticizing pressures' alone are insufficient for explaining the EU's embrace of a geopolitical, sovereigntist and/or open strategic autonomy approach (Haroche, 2023; Baracani & Kassim, 2024; Juncos & Vanhoonhacker, 2024). As Baracani and Kassim (2024) point out, the same geopolitical tensions which had contributed to the

Commission's geopolitical 'success' over the 2019-2023 period could conceivably exacerbate future *dissent* across Member States, EU institutions, and European publics. After all, the EU's digital sovereignty and geopolitical ambitions have been dogged with areas of incoherence and inconsistency between the Union's aspirations and its capabilities, including the relationship between digital sovereignty discourse and EU cyber policy changes (Carver 2024b). Even within the *same* EU policy domain, geopoliticization has 'manifest[ed] differently' (Herranz-Surralléz et al., 2023, p. 925; see also Carver 2024b). Indeed, endogenous factors specific to the EU's institutional context, including the ambitions of various EU actors, have also played an important role in mediating the EU's geostrategic turn (Juncos & Vanhoonhacker, 2024; Baracani & Kassim, 2024; Csernatoni, 2022).

Departing from these limitations, critical scholars have underscored the complex sociotechnical nature of cyberspace (Dunn Cavelty & Wenger, 2022) and the relationship between securitization and actors' imaginaries of the strategic environment (Backman, 2023; Monsees & Lambach, 2022), which could further explain the EU's particular approach to geopolitics and sovereignty in cyberspace. While this scholarship has equivocated that ontological security drives, including identity and reputational concerns, may mediate strategic behaviour in cyberspace (e.g. Smith, 2023; Herranz-Surralléz et al., 2023; Bellanova et al., 2022, p. 348; Lupovici, 2023), it has failed to elaborate the ontological security foundations of the EU's geostrategic turn.

Meanwhile, there have been few attempts by the literature to examine how spatial (b)ordering practices may have shaped the development of the EU's self-image over time, even in critical scholarship (cf. Smith, 2023; Lambach, 2020; Branch, 2017). From a material perspective, scholars have explored how the structural features of cyberspace shape states' strategic behaviour (e.g. Foulon & Meibauer, 2024; Maschmeyer, 2023; Fischerkeller

et al., 2022), although they have failed to rigorously examine how this behaviour relates to spatial (b)ordering practices—a much wider phenomenon (Lambach, 2020).

As I argue below, political geography and critical geopolitics scholarship on cyberspace provide rich analytical tools for moving beyond Westphalian/non-Westphalian debates about the structural features of cyberspace and their connection to geostrategic concepts. Departing from these insights suggests that, beyond material consequences, spatial (b)ordering in and through cyberspace is potentially underpinned by ontological security drives.

Uncovering the relationship between spatial (b)ordering and ontological security behaviour in cyberspace

Emerging in parallel to mainstream cyber-IR (Lambach, 2020), critical geopolitics and political geography literature conceives of spatial (b)ordering practices as a much broader phenomenon than classical 'Westphalian' IR paradigms. Classical Westphalian approaches to spatiality in IR imagine territoriality as a 'state-force-territory' relation, forming the basis of orthodox sovereigntist and geopolitical concepts (Agnew, 2008; Barkawi, 2016, p. 207). As reviewed above, mainstream cyber-IR has tended to position 'cyberspace' as awkwardly straddling a Westphalian/post-Westphalian dichotomy, given widespread recognition that it cannot be 'essentialized' into either category (Lambach, 2020; Balzacq & Dunn Cavelty, 2016).

However, positioning Westphalian concepts as either the foil or foundation of cyber power runs the risk of reproducing the 'territorial trap' in cyber-IR, eliding the co-constitutive nature of digital technologies and social imaginaries across multiple scales and relationalities (see also Lambach, 2020; Acemoglu & Johnson, 2023). For example, while scalar (networked) accounts of cyberspace have often tended to assume 'flat' or distributed

power relations (as the antithesis of traditional territoriality), networks and territories can be compatible and mutually constitutive (Lambach, 2020; see also Carver, 2024a).

Valuably, critical geopolitics and political geography literatures conceive of spatial (b)ordering practices as both *producing* and *demarcating* space through ideas, practices, and institutions (Lambach, 2020; Branch, 2024; see also Simmons & Hulvey, 2023). In cyberspace, spatial (b)orders comprise 'technopolitical assemblages of hardware/infrastructure, code, data, and social relations' (Lambach, 2024, p. 296) which govern relations of circulation and control (Zhang & Morris, 2023). Accordingly, spatial (b)ordering moves in cyberspace are understood as 'attempt[s] to engineer differences' (Simmons & Hulvey, 2023, p. 9), comprising the ideas, practices, and technologies of demarcation (Branch, 2017).

Accordingly, this draws our attention to '*the production of space*'—that is, 'how places are socially and materially created, reconfigured and experienced' in various contexts (Cloke, Crang, & Goodwin, 2014, p. 940; in Weaver, 2020, p. 2). Relevant to the EU's geostrategic turn, this approach emphasizes that spatial (b)ordering practices—including in cyberspace—do not necessarily reproduce traditional territorial state boundaries, but they also provide opportunities for actors to challenge existing modes of global spatial order (see also Mueller, 2020; Branch, 2024, p. 310).

Further, approaching spatial (b)ordering through this perspective makes it possible 'to ask how practices constitute digital territories and how these territories impact *future* practices' (Lambach, 2024, p.99, emphasis my own). Indeed, the process of delimiting and demarcating EU borders lies at the heart of the European integration project (Schimmelfennig, 2021)—thus foundational to upholding and/or reconstructing the EU's existence over time (see also Fassi et al., 2023; Agnew et al., 2017; Diez, 2004). Elsewhere, scholars have argued that spatial (b)ordering practices may be deployed to manage an actor's

ontological security needs, including upholding an actor's sense of self over time (Eberle & Daniel, 2022; Agnew, 2004; Browning, 2018; Mitzen, 2017, p. 414). Thus, such 'spatialised readings' of power relations (Weaver, 2020) emphasize the *constitutive* nature of spatial (b)ordering for an actor's sense of self and their capacity to project power, including in and through cyberspace.

From this perspective, it is striking that cyber-IR scholarship has widely equivocated yet scarcely explored the ontological security dimension to strategic behaviour in cyberspace and its potential relationship to spatial (b)ordering practices (e.g. Herranz-Surralléz et al., 2023; Liebetrau & Christensen, 2021; Malksöo, 2018; Lupovici, 2023). The distinctive ontological challenge posed by cyberspace is first exposed by its variable and contested definition (Branch, 2024; Lambach, 2020). Cyberspace is characterized by an ambiguous geographic context wherein 'technology, organizations, and skill are not easily separable variables (Slayton, 2016, p. 83). Ontological challenges about 'what exists' in cyberspace have not only been recognized by a longstanding securitization literature on cyberspace (see for example Hansen & Nissenbaum, 2009; Christou 2013, 2016; Balzacq & Dunn Cavelty, 2013), but they are also reflected in practice. Across the world, and over time, policymakers have advanced varying definitions of cyberspace and the digital domain (Betz & Stevens, 2013; Creemers, 2024; Carver, 2024b; Broeders et al., 2019), demonstrating that they are often considered to be transversal political and strategic environments (Carver, 2024a).

IR scholarship has observed that ontological challenges posed by cyberspace, including the domain's complex relationship to territorial borders, have shaped how policymakers behave (e.g. Lonergan & Schneider, 2023; Betz & Stevens, 2013; Gomez, 2019). Indeed, widespread ontological dissensus about the basic features of the 'cyber domain', the 'virtual battlefield', and/or 'cyberspace' lays bare the constructed, subjective, and potentially irrational groundings of geospatial analogies applied to cyberspace (Betz &

Stevens, 2013). As Branch surmises, despite—or perhaps *because* of these conceptual challenges—'The intuitive appeal and rhetorical power of the spatial metaphor implicit in cyberspace may simply make it too tempting to avoid,' (2024, p. 310).

Accordingly, this scholarship suggests that spatial (b)ordering practices, and their relationship to ontological security seeking drives, may play a greater role in shaping actors' geostrategic behaviour than is currently accounted for by mainstream cyber-IR theories. Relevant to the case of the EU, this literature has also alluded an influential relationship between ontological security drives, bordering practices, and the EU's geostrategic turn in and through cyberspace.

Theoretical framework: Spatial ordering, bordering practices, and ontological security in and through cyberspace

How, then, has the EU's engagement with spatial (b)ordering practices in cyberspace shaped its evolution as a (geo)strategic cyber actor, and to what extent have ontological security drives underpinned this relationship?

To approach these questions, I develop a theoretical framework centered around the relationship between *spatial (b)ordering practices*, the Union's *ontological security drives,* and its development as a global cyber actor. This framework theorizes that the process of constructing the EU's role as a global cyber actor has been constituted by spatial (b)ordering moves, which have been underpinned by the Union's search for ontological security. Specifically, I argue that spatial (b)ordering moves have attempted to stabilize the EU's self-representation as a global actor in cyberspace through three pathways: 1) *routinized spatial (b)ordering strategies*; 2) *discourses of demarcation*; and 3) *spatial adaptations*.

I understand the EU as a collective actor 'in the making' (Mitzen, 2018), premised upon the Union's 'capacity to imagine and realize roles for its Self,' in a particular policy context (Klose, 2018, pp. 1145-47; for a similar approach, see Smeets & Dunn Cavelty,

2023; Flockhart, 2020). Accordingly, the EU's evolving actorness in cyberspace is conceived as a process shaped by both internal and external social contexts which 'emerges from the interplay of (domestic and external) role expectations, creative action and (social and material) resources' (Klose, 2018, p. 1145). By conceptualizing the EU as a collective actor, I build upon an established area of ontological security studies applied towards the EU (see for example Mitzen, 2018a,b; Lupovici, 2023; Browning, 2018; Zarakol, 2017).

Ontological security and 'the capacity to act' in and through cyberspace

First, I theorize that the EU's process of constructing its role as a global cyber actor has not only been influenced by material security concerns, but by its ontological security seeking behaviour—that is, the 'active process of constructing the self and anchoring it in the social world' (Eberle & Daniel, 2022, p. 2). This builds upon the insights from ontological security studies (OSS), which has emphasized that 'states care as much about their ontological security, *the security of a consistent self*, as about material, physical security, the traditional purview of IR inquiry,' (emphasis my own; Subotic, 2016, p. 614; see also Krickel-Choi, 2021).

Managing one's ontological security is crucial for an actor's sense of agency (Flockhart, 2016) and their 'capacity to imagine and realize roles for its Self' (Klose, 2018, p. 1145)—thus giving their actions and decisions meaning (Subotic, 2016). Engaging in predictable and secure routines with significant others enables actors to pursue autobiographical continuity, and in turn, a more stable identity (Subotic, 2016). For foreign policy actors, this is often achieved by constructing self-reflexive *discourses,* such as 'autobiographical identity narratives', which link an actor's identity with the 'good past', a process which helps them to reinforce their identity and make sense of their current behaviour, including their relations with others and position in the global environment

(Subotic, 2016, p. 614). Ontological security management strategies are also pursued through self-affirming *practices,* such as reproducing the boundaries of the 'contained self' vis-à-vis others in a given context, for instance by (re)establishing familiar social and/or territorial boundaries (Mitzen, 2018b; Lambach, 2024).

Thus, the search for ontological security can be understood as 'a reflexive project of continuously seeking to maintain a sense of "self" through "being' and "doing" *in a constantly changing environment*,' (Flockhart, 2016, p. 805, emphasis my own). Critically, changing environmental conditions and/or social relations may introduce 'problematic situations' for actors which 'challenge established routines' central to reproducing their roles in a given context (Klose, 2018, p. 1148).

Ontological security scholarship has empirically demonstrated that ontological insecurities may be autobiographical (Flockhart, 2016; Kinnvall & Mitzen, 2020), relational (Cash, 2016; Diez, 2004), spatial/geographical (Browning, 2018) or a combination thereof (Browning & Joenniemi, 2017). Building upon this work, I conceptualize three loci of ontological insecurity relevant to cyberspace.

Theorized loci of ontological insecurity in and through cyberspace

As argued in the previous section, it is plausible that acting in cyberspace can elicit ontological insecurities for reasons related to the domain's environmental attributes; socio-political dynamics of strategic uncertainty and lack of trust in the nature of relations between cyber actors; and the domain's complex relationship to an actor's physical territoriality and sovereignty. As Malksöo avers, cybersecurity issues 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' (2018, p. 378). Indeed, scholarship has widely demonstrated that foreign policymakers

contend with strategic uncertainty, cognitive biases, (ontological) anxiety, and fear in their efforts to provide cybersecurity and advance strategic objectives in and through cyberspace (Gomez, 2019; Betz & Stevens, 2013; Gomez & Whyte, 2021; Dunn Cavelty & Wenger, 2021; Branch, 2017; Lonergan & Schneider, 2023; McDermott, 2019).

Building upon this work, I theorize that cyberspace may induce *autobiographical* (or self-reflexive) ontological insecurities, as 'cyber technologies complicate states' ability to maintain the borders that define the (national) home', and therefore, a coherent autobiographical narrative (Lupovici, 2023, p. 161). Recent global crises, including the COVID-19 pandemic and the influence of private sector actors, have further underscored the 'hybridization' of digital/virtual space with physical space, complicating states' capacity to maintain their privileged roles as sovereign actors and security providers (Lambach, 2024; Blancato & Carr, 2024). Indeed, state-based actors have traditionally linked their sense of Self with state-based territoriality and sovereignty, whereby 'the claiming, delineating and protecting of territory' has served as a key way for actors to imagine themselves as 'whole' (Krickel-Choi, 2022b, p. 170; Mitzen, 2018). Notably, this sentiment has been recently expressed by the EU in terms of 'European sovereignty', as conveying the EU's desire to 'act' autonomously in the world (Costa & Barbé, 2023).

Furthermore, cyber insecurities may trigger *relational* ontological insecurity for foreign policy actors, due to the high degree of uncertainty about others' behaviour and the 'rules of the game' in and through cyberspace (Nye, 2016; Aleksandrowicz, 2015). That is, lack of trust in the 'rules of the game' and in the predictability of relations with external Others may challenge EU policymakers' 'framework of reality' and thereby their capacity to (re)imagine an EU global role in and through cyberspace.

Finally, the territorially complex and rapidly evolving characteristics of cyberspace could generate ontological insecurities relevant to the *environment,* as the domain's

'borderless', fluid, 'virtual layer' may create a rift between an actor's 'spatial understanding of the world' and an actor's capacity to imagine oneself as 'whole,' a process sustained by collective recognition of an actor's borders and authority (Krickel-Choi, 2022b; Della Sala, 2017).

These theorized loci of ontological insecurity relevant to an actor's self in the context of cyberspace are visualized in Figure 6.1.

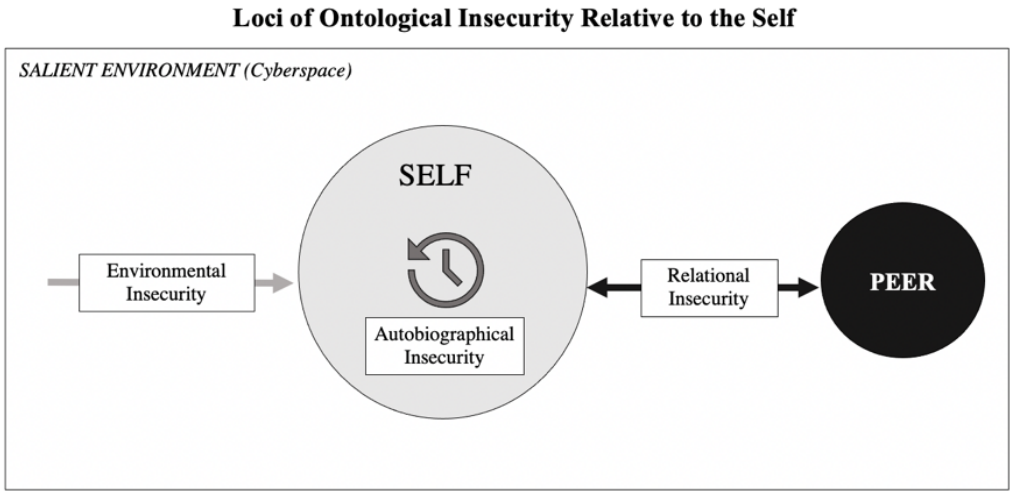


Figure 6.18. Theorized triggers of ontological security seeking behaviour relevant to the EU's existence as a global cyber actor.

These potential triggers of ontological insecurity suggest that constructing a role in and through cyberspace may destabilize the EU's efforts to establish coherence between its spatial and political architecture(s), its historical self-narrative, and a clearly defined European spatial imaginary. In turn, as I argue in the next section, political actors seek to manage ontological insecurities through various strategies, including various discourses and practices of spatial (b)ordering.

Spatial (b)ordering practices as ontological security (OS) seeking behaviour

Following OS theory, experiencing ontological insecurity is theorized to trigger *ontological security seeking* behaviour, whereby an actor seeks to stabilize its 'Self' through a 'certain [creative] course of action,' (Klose, 2018, p. 1147). Significantly, OS seeking behaviour can manifest as 'spatial (b)ordering' moves (Browning, 2018), which consist of ideas, practices, and technologies of demarcation (Branch, 2017; see also Weaver, 2020, p. 3). Under conditions of ontological insecurity, spatial (b)ordering moves broadly attempt to locate and *emplace* an actor's self, thereby 'captur[ing] a sense of being' in the world and vis-à-vis relational others (Browning & Joennimi, 2017, p. 34). In this way, spatial (b)ordering moves may seek to secure the Self or bring stability to an actor's surroundings and/or their relations with others.

Building upon this scholarship, I theorize that spatial (b)ordering practices enable actors representative of the EU to pursue three interrelated ontological security (OS) seeking strategies in and through cyberspace: 1) *routinized spatial (b)ordering strategies; 2) discourses of demarcation*; and 3) *spatial adaptations*. These are elaborated below.

Routinization to stabilize the Self

First, I expect that ontological insecurities about one's relative position and authority in cyberspace (e.g. a perceived loss of agency and/or sovereignty) can encourage *routinized* self-narratives (Flockhart, 2020, p. 219; see also Hagström, 2021, p. 334). Self-affirming narrative routines may entail the reification of territorial borders in and through cyberspace, and the use of (geo)spatial analogies which reproduce an actor's positioning vis-à-vis others and its authority over its territorial borders in digitalized contexts (Lambach, 2024). For example, actors may engage in threat externalization, premised upon constructing the *inside*

of the self as a place of safety ('home') and *outside* of the self as insecure and disorienting (Mitzen, 2018, p. 1379), as a form of bordering.

Equally, routine spatial (b)ordering practices may be deployed to bring order to a disorienting and ontological complex external environment (see also Eberle & Daniel, 2022). Analogizing cyberspace to territorial borders, Branch argues,

> 'gives actors the ability to make comprehensible what might otherwise be impossible to grasp: the implications for state authority and sovereignty—defined in terms of physical territory and demarcated boundaries—of cyber threats and challenges that are inherently boundary-crossing (2024, p. 301).'

However, alongside narratives and discourses, routinization can also be achieved through spatializing practices and policy instruments. Elsewhere, scholars have shown that the EU has sought to embed itself and its normative preferences abroad by engaging a variety of soft and hard (economic) policy instruments directed toward its Neighbourhoods in concentric circles (Bialewicz, 2015; Cadier, 2019; Browning, 2018). Such (routine) bordering practices 'reflect, re-enact and routinize a particular conception of self-identity premised upon a particular understanding of the nature of its salient environment,' (Browning, 2018, p. 107). Overall, by transposing existing spatial routines from other domains in and through cyberspace, actors may seek to reconfigure (physical) space or territorial boundaries in line with an actor's imaginary of their self, thereby managing a dislocation between 'envisioned' and 'experienced' space (see also Lupovici, 2016).

Discourses of demarcation vis-à-vis a significant Other

Relatedly, spatial (b)ordering moves may constitute *discourses of demarcation,* or 'othering', a widely recognized form of ontological security management behaviour (Mitzen, 2018; Browning, 2018). As an ontological security management strategy, demarcating the Self's attributes in opposition with that of a significant 'Other' constructs an actor's identity as meaningful, legitimate and credible (Browning & Christou, 2010),

helping to assuage ontological insecurities about one's Self relative to others. Indeed, bordering narratives which 'define and locate the self in the social world' *vis-à-vis others* are a primary mode of managing ontological insecurities (Mitzen, 2018, p. 1374; Laine, 2020; Mills, 2014).

Spatial adaptation to manage ontological disruptions

Lastly, I expect that the productive nature of spatial (b)ordering may facilitate opportunities for *spatial adaptation* (Flockhart, 2020; Klose, 2020). In this way, spatial (b)ordering moves may be deployed to re-envision actor's role under conditions of ontological disruption and insecurity (see also Krickel-Choi, 2022a).[63]

Thus, in line with the recent wave of OS scholarship (e.g. Flockhart, 2016, 2020; Rumelili, 2015; Krickel-Choi, 2022a), this framework remains open to the possibility that ontological security imperatives may inspire adaptation, not only stasis, in the EU's global role construction. This reflects the evolving character of the EU's constitutive *political* identity (Habermas, 1996; see also Mitzen, 2018, p. 398) and it recognizes the possibility of there being multiple potential EU identities up for negotiation vis-à-vis the EU's collective 'Self' (see also Diez, 2004, p. 321; Klose, 2022; Cash, 2016; Csernatoni, 2022). Indeed, the progression of European integration has led to the EU's consequential adoption of new characteristics and competences over time, most recently evidenced by the policy domain of cybersecurity (Carrapico & Farrand, 2024).

[63] Earlier ontological security scholarship has been criticized for its tendency to presuppose stasis as opposed to change in policymakers' behaviour under conditions of insecurity. 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 (see Cash, 2020). 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, refuting that ontological security does not necessarily equate to the search for fixity or consistency of identity (Kinnvall & Mitzen, 2020). 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 (Mitzen, 2018a, p. 398).

Notably, these strategies are not mutually exclusive but idealized types. They are expected to manifest by various EU actors in different ways and/or combinations. For example, routinized self-narratives may habitually engage with 'Othering' discourse to construct an actor's self in opposition to a familiar set of attributes. Similarly, actors may selectively engage with routinized practices and spatial adaptation moves to manage the dislocation between a new role conception and an actor's historical Self (see also Klose, 2018; Subotic, 2016). Subotic puts it thus,

> 'As [actors] move through international society, enter new relationships with other [actors], and experience momentous events, their stories change and incorporate new elements. This does not necessarily mean that [an actor's] narrative, its autobiography, must be fundamentally altered. Instead, new events are interpreted in line with specific elements of the narrative, emphasizing some aspects of the narrative and disregarding others,' (2016, p. 614).'

These theorized strategies are represented in the below table.

Table 6.9. Summary of theorized relationship between bordering practices and ontological security drives in EU policy behaviour.

Spatial bordering practice	**OS seeking strategy**	**Explanation**	**Indicative example**
Routinization	Adopt familiar 'routines' to new locale Securitization of the self	Transposition of existing spatial logics onto new environment/domain in discourse and practice Threat externalization: Constructing the inside of the self as a place of safety ('home') and outside of the self as insecure and disorienting	Reproducing familiar narratives about the Self in X, in new context Y to justify actions (i.e. 'I have been a longstanding leader in X and this is no different when it comes to Y")
Discourses of demarcation	Geopolitical othering	Describing the self in diametric opposition to a relational Other.	"I am X, s/he is not-X."
Spatial adaptation	Adapt self-positioning in various spatial contexts to cohere with reconceptualized self-imaginary	Adoption of new territorial logics and practices to cohere with adapted self-representation	Adopting a new discourse of 'digital sovereignty' and policies which seek to operationalize the concept in cyberspace for the first time

Overall, given that cyberspace embodies a constantly evolving and complex environment, constructing an EU global role in this domain may be fraught with multiple 'problematic situations' which could trigger a host of different ontological insecurities. Thus, I expect that spatial (b)ordering practices have been crucial for (re)imagining the EU's role in and through cyberspace over time. In line with the expectations of OS scholarship, OS management strategies are not expected to guarantee or fully satisfy the EU's ontological security needs. As scholars have demonstrated elsewhere, efforts to better 'locate' the self through spatial (b)ordering and role adaptations may introduce further tensions, paradoxes, and insecurities in the actor's self-representation (Subotic, 2016; Krickel-Choi, 2022b; Klose, 2020, p. 852). Equally, ontological security-seeking behaviour may also complicate an actor's response to material security concerns; when a material security concern is also perceived as an existential threat, an actor may compromise aspects of their material security in order to cope with the ontological insecurity (Subotic, 2016; Wendt, 1994). Thus, I conceive of the EU's quest for ontological security as ongoing, in line with the discursively constructed and potentially contested nature of the EU's actorness (Diez, 2004; Mitzen, 2018; see also Hagström, 2021).

Analytical approach

To probe the plausibility of my framework in the case of the EU's geostrategic turn in and through cyberspace, I adopted a qualitative-interpretivist analytical approach, which enabled me to analyse the relevant constitutive ideas, practices, and resources underlying the EU's role construction in and through cyberspace over the 2009-2024 period (Schwartz-Sea & Yanow, 2012; Moisio & Paasi, 2013). By emphasizing the constitutive nature of discourses and practices (Schwartz-Shea & Yanow, 2012), an interpretive-qualitative

approach is well placed to grasp the evolving sociotechnical nature of cyberspace and uncover the EU's engagement with spatial (b)ordering and ontological security drives.[64]

To identify and contextualize various (competing) internal imaginaries about the EU's role construction as a (global) cyber actor over time, I conducted a discourse analysis of over 100 primary source documents (mostly drawn from the EURLEX database)[65] and 21 formal and 5 informal elite interviews[66] of relevant policymakers in EU institutions (European External Action Service, European Commission, the Council of the European Union), and two current/former Member States (viz. the United Kingdom, Estonia, and Lithuania), as well as relevant external organizations (Council of Europe, Global Cyber Security Capacity Centre, and the European Union Institute for Security Studies) (see also Appendix A). This empirical timeframe covers the empowerment of the EU's diplomatic services (EEAS), in 2010, the release of the EU's first ever cybersecurity strategy (in 2013), and the EU's most recent and active cyber strategy, *The EU's Cybersecurity Strategy for the Digital Decade* (2020), as well as more recent strategic developments pertinent to the EU's external action role, viz. the EU's *Strategic Compass* (2022) and internal cybersecurity issues, viz. the *NIS2 Directive* (2023) amongst others.

---

[64] This also accounts for the fact that the EU cyber-external action policy context has been characterized by the reconceptualization and mainstreaming of digital and cyber issues over time (see also Carver 2024a; Liebetrau, 2024; Farrand et al., 2024. Digital and cyber policy areas have historically overlapped, including in the areas of cyber/digital diplomacy (Renard, 2018), cyber defence (Csernatoni, 2022), and critical infrastructure protection (European External Action Service, 2021; see also Carrapico & Farrand, 2024). In civilian policy contexts, 'cyber' issues are currently considered to be 'enablers' for the EU's *digital* policy agenda, which is regarded as a more encompassing policy domain (Barrinha & Christou, 2022; Bellanova et al., 2022).

[65] My data corpus included *inter alia* strategic documents, parliamentary resolutions, EU regulations, blog posts, meeting minutes, reports, and speeches produced by the European Commission, the Council of the EU, the EEAS, ENISA, the European Parliament (EP), the European Court of Auditors, the cybersecurity and defence private sector. Additionally, I examined, where possible, national parliamentary debates about EU proposals, public surveys, and EU Staff Working Documents.

[66] The author obtained approval for conducting research with human participants from the DPIR Departmental Research Ethics Committee (DREC) in accordance with the procedures laid down by the University of Oxford for ethical approval of all research involving human participants, and informed consent from all interviewees. Ethics approval reference numbers are SSH_DPIR_C1A_21_005 and SSH_DPIR_C1A_22_008. Due to the politically sensitive nature of the research and in line with interviewee consent, interview data cannot be made openly available. However, the archival sources used by the study are openly available, accessible at the EURLEX database and as noted in the reference section of the paper.

My empirical analysis comprised two interrelated and recursive steps. First, I examined how the EU has constructed its Self as a cybersecurity actor in global cyberspace over time (2009-2024), with a focus upon various spatial (b)ordering discourses and practices. Second, I probed whether such practices appeared to reflect the Union's efforts to manage ontological insecurities in this context, such as dislocations in the EU's self-image or relational insecurities about the outside environment, as laid out in my theoretical framework.

First, my analysis began by exploring discourses relevant to 1) the creation of the EU's role in cyberspace in the 2013, 2017, and 2020 cyber strategies and 2) the EU's global approach (e.g. the Union's security and foreign policy strategies). I identified relevant actors, issues, and further source materials associated with these strategic documents by engaging in intertextuality, which entails 'situating texts within and against other texts to reveal how one particular source (e.g., a strategy document) is embedded within the broader political and social discourse,' (Schwartz-Shea & Yanow, 2012, in Carver 2024b, p. 2258).

To explore how, if at all, various EU actors perceived an ontological security dimension(s) to the Union's strategic approach to cyberspace, my analysis drew upon Bacchi and Goodwin's interpretive tool, 'What is the Problem Represented to Be' (WPR Analysis). WPR analysis consists of a series of critical questions about the problem emphasis and policy prescriptions and/or solutions linked to it. By examining how issues are framed as *particular* problems, I scrutinized how EU actors 'interpret[ed] information by promoting a particular problem definition, causal interpretation, moral evaluation and/or treatment recommendation,' (Christou & Damro, 2024, p. 1082). Drawing upon my theoretical framework, I consider empirical indicators of ontological insecurity to include (cybersecurity) problems framed in existential terms, such as issues explicitly linked to EU identity and its functioning as a political actor; problems which demand a 'fundamentally

different' ontological approach/orientation to make sense of the world and/or actors within it; and problems linked to the EU's foundational self-narrative as an actor.

Alongside probing for observable evidence of ontological insecurities in this data corpus, I critically examined how various EU policy communities constructed the EU's autobiography in and through cyberspace and vis-à-vis others. Particularly, I focused upon identifying various EU self-narratives in documents and interviews and the particular role(s) they prescribed for EU external action in this context. This was an iterative process during which I identified areas of repetition in EU cybersecurity discourses across different texts (intertextuality), institutional contexts, and over time. To inform this analysis, I also considered insights of wider EU studies. This literature has emphasized the significance of the EU's explicit eschewal of geopolitics as a 'founding myth' constituting its origins as a *sui generis* actor (Guzzini, 2012; Fisher Onar & Nicolaïdis, 2015), together with the EU's 'values-based' and/or 'civilizational identity' (Zielonka, 2011) and the Union's historical self-positioning as a global 'technological leader' (Monsees & Lambach, 2022).

Altogether, this analysis concentrated on various supranational and intergovernmental discursive contexts at the EU level to identify discursive struggles over the EU's role as a global cyber actor at both the horizontal (i.e. across EU institutions) and vertical (between Brussels and Member States) levels. Alongside high-level strategic debates around the EU's global role in cyberspace, I examined how the EU positions itself externally vis-à-vis third countries by focusing upon the policy areas of cyber-relevant strategic partnerships, capacity building, and (international) development cooperation, two significant areas of EU external action in cyberspace (Carver 2024a,b). Examining these dynamics is reflective of the development of EU cyber-external action policies over 2009-2024 (see also Carver 2024b; Laurer & Seidl, 2021; Timmers, 2018; Pawlak, 2018; Trimintzios et al., 2017, p. 5; Heidebrecht, 2024).

Ultimately, this paper seeks to understand the potential relationship between bordering practices, ontological security drives and the EU's evolving strategic behaviour in and through cyberspace. This approach, I argue, will improve our understanding about the Union's quest to take on a geostrategic role in global affairs, particularly in the context of cyber-external action. However, it should be noted that the policy contexts and issues examined here are not representative of *all* social processes leading to the construction of the EU's role in and through cyberspace.

By exploring these dynamics through a qualitative-interpretive perspective, the purpose of the article is not to falsify existing accounts of the EU's geopolitical turn or to provide a complete or universal theory about the EU's actorness in cyberspace. Rather, this article seeks to examine how material and ontological security concerns may theoretically co-exist and potentially compete with each other in the context of cyberspace (see also Flockhart, 2020; Subotić, 2016). Nor is the aim of this study to conclusively identify what kind of actor the EU is; this topic has been widely discussed elsewhere in terms of EU's normative (Manners, 2002), civilian (Bull, 1982), market (Damro, 2012), and liberal (Wagner, 2017) identities, among others. Instead, I expect that the EU's role in and through cyberspace will evolve over time, in keeping with how policymakers conceptualize and 'border' the domain itself. After all, as Manners and Whitman (2003) argued, the EU is constituted by an 'expectation of territorial change' (in Mitzen 2018b, p. 1383).

By anchoring the analysis around major changes to the EU's strategic approach to cyberspace (*inter alia* the 2013, 2017, and 2020 cyber strategies), and by examining how the EU's role(s) have played out in various contexts of the EU's cooperation with third countries, this study offers the first in-depth exploration of how spatial (b)ordering and ontological security imperatives appear to have shaped the EU's (geo)strategic development as a cyber actor. Moreover, it seeks to advance our theoretical understanding of geostrategic

behaviour in cyberspace by introducing sociopsychological and critical geopolitical tools to explore these dynamics. It is to this analysis that I now turn.

Empirical analysis

Below, I illustrate how various EU actors have engaged in spatial (b)ordering moves in cyberspace to demarcate, legitimize and consolidate the EU's role as a global cyber actor over time. Moreover, spatial (b)ordering moves have sought to manage the Union's ontological security—and fundamentally the Union's sense of agency—in an evolving strategic environment.

Background: Constructing a European cyberspace, 2009-2013

In the early post-Lisbon years, managing cross-border and 'borderless' cyber insecurities were prevalent issues in both horizontal and vertical debates over the EU's first proposed cyber strategy. Throughout this timeframe, key EU institutions appealed to both existential and material security concerns to construct a legitimate EU role in 'borderless' cyberspace. Establishing the boundaries for EU action in 'borderless' cyberspace during the 2009-2013 period laid the basic conceptual (and political) foundations for the Union's global role in later periods.

Specifically, the years leading up to the EU's first cyber strategy saw growing Europeanization and harmonization of Member States' policies towards cyberspace, in part driven by the urging of the European Commission (Nielsen, 2012; Klimburg & Tirmaa-Klaar, 2011). However, the issue of *cybersecurity* 'remain[ed] almost exclusively a national prerogative' (Renard, 2014, p. 13; in Carrapico & Barrinha, 2017, p. 1266). In 2009, 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. Skepticism about whether it was 'sensible to develop European-centric approaches at all' (United Kingdom Cabinet Office, 2009), is illustrated by policy debates in the United Kingdom, one of the most capable or 'cyber-mature' Member States at the time. Written evidence given by the Cabinet Office to the House of Lords in 2009 illustrates parliamentary witnesses' 'widespread reluctance' to demarcate an EU-level role:

> '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 (in European Union Committee, 2010, p. 17).'

The UK government's statement envisioned EU action in cyberspace as confined to internal *European* matters and discourages the EU's involvement in *global* cyberspace as a security actor. London justified this position on the grounds that 'the Internet operates as a global phenomenon and *does not recognise borders*,'—therefore, cyberspace does not inherently warrant a European-centric focus (European Union Committee, 2010, p. 17, emphasis added by author).

A European 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,' (Mr Servida, in European Union Committee, p. 17). By this account, the EU's role as a security coordinator and rules-setter was framed as not only valuable, but *necessary* for the ability of all European (Member) States to survive in cyberspace. In turn, London conceded that *some* form of EU role was 'legitimate' given the risks of 'cascaded failure' in cyberspace, but it was still deemed 'second best' to a global orientation (European Union Committee, 2010, p. 143; see also House of Lords, 2011, p. 11; Home Office, 2010, pp. 2-5).

Nonetheless, prior to the publication of the 2013 strategy, the Council of the EU conceived of cyberspace as *space controllable by states,* asserting that states should 'protect that part of cyberspace for which they are responsible,'(General Secretariat of the Council & EUISS, 2009, p. 7) Thus, while the Council expected cybersecurity challenges to cross the internal/external dimensions and pillars of the EU due to its cross-border nature, the Council effectively transposed European states' national territorial sovereignty onto cyberspace.

Yet, cyberattacks during this period, including Stuxnet (2010) and a 'serious' cyberattack against the Commission and the EEAS' in 2011 underscored the Union's potential vulnerabilities to insecurities in and through cyberspace (Vogel, 2011; Interviewees A, B, C, F), albeit through an economic security perspective (see also Whyte, 2021). However, the issue of cybersecurity was not considered a priority for the EU's *global* and foreign policy agendas (Klimburg & Tirmaa-Klar, 2011). For some Member States such as the UK, external representation by the EU remained a contentious issue (House of Commons European Committee B, 2013). As such, prior to the 2013 strategy, 'the European External Action Service (EEAS) [had] not yet proactively included a cyber security aspect in its relations with third countries,' (European Parliament, p. 147). Consequently, a study by the European Parliament summed up the situation as:

> '[A] near total lack of CFSP engagement in this topic – as well as weak coordination among the EU institutions themselves – have meant that the ability of the EU to measurably project 'cyberpower', or even deal with serious cyberattacks, is very limited indeed,' (Klimburg & Tirmaa-Klaar, 2011, p.4).

In this context, official EU debates about cybersecurity issues largely omitted geopolitical threat representations (Interviewees A, B), and official EU engagement with geopolitical or 'cyberwarfare' concepts was implicit (European Commission, 2009) or notably absent from EU cybersecurity documents during this timeframe (see also Klimburg & Tirmaa-Klaar, 2011; European Parliamentary Research Service, 2013). This may be

contrasted with the visibility of these issues at the Member State level, as seen in national level responses to multiple significant cyber events in the noughties, including Stuxnet, disinformation, and 'botnets' (see also Klimburg & Tirmaa-Klaar, 2011, pp. 11, 26). For example, the 2007 denial-of-service cyberattacks on Estonian critical infrastructure were attributed by some EU Member States as a *geopolitically motivated* attack by Russia (Interviewee B; F; Pamment et al., 2019, p. 56; Douzet, 2014, cf. European Parliament, 2007) and a NATO-wide response was debated at the time (Ansip, 2007; Traynor, 2007). By contrast, 'geopolitical' discussions about cyber insecurities were invisible at the EU level in this context until years later (Interviewees A, C). This reflects one EU policy expert's belief that, until very recently, the EU had never really considered its *own* actions in geopolitical terms (Interviewee C).

Rather than emphasizing geopolitical threats, supranational EU institutions framed cybersecurity risks in terms of the EU's historical role as an economic and political security provider. Up until 2013, the Commission and the European Parliament repeatedly expressed how cybersecurity and data protection measures were seen as crucial for 'complet[ing] the single market:' a foundational construct for the EU's existence as a political and economic bloc (Barroso, 2012; see also European Parliament, 2010; 2013; European Commission, 2011b; 2013a). For example, in the 2010 *Digital Agenda for Europe,* the Commission described cyberspace as a 'borderless' domain and reasoned that online barriers to markets should be struck down (2010, p. 4). However, it also recognized the strategic importance of the internet and the necessity for including an *external dimension* to cybersecurity to preserve a European 'digital way of life' (pp. 5, 34). Thus, ensuring that the EU managed issues of public trust and cybersecurity risks pertinent to the Internal Market was seen as crucial for the EU's credibility to its citizens, and fundamentally, the Union's *raison d'être.*

Linking cybersecurity issues to economic security and the EU's existence reproduced similar narratives in other areas of EU policy during this period. Particularly, the 2008-2010 Euro crisis had exposed flaws in the functioning of the EU's internal market and plunged Brussels institutions into a 'crisis of confidence,' (Barroso, 2012). The Eurocrisis, after all, was conceived as not merely an economic security issue, but a *political* 'problem of credibility' in which citizens were made to 'feel their way of life is at risk,' (Barroso, 2012; see also Whyte 2021). Given the wider context of the Union's 'crisis of confidence' post-Euro crisis, the routinized approach undertaken by EU supranational institutions towards cyberspace indicates shared anxieties about the EU's capacity to fulfil its historical role as an economic security provider and as fostering trust in the EU's existence as a political project.

Furthermore, documentary evidence suggests that EU institutions engaged spatial (b)ordering moves to manage these autobiographical insecurities. By drawing upon familiar narratives and routines about European 'core values', a 'single European [information] space' (e.g. European Parliament, 2010), and the security of the Internal Market, the EU's role and territorial imaginary was reproduced in cyberspace. EP resolutions from this period adopt a similar characterization, constructing an *EUropean* imaginary of borders in cyberspace characterized by a harder external (non-European) border with fluid/weak internal barriers (European Parliament, 2012; 2013, p. 114).

Ultimately, dissensus about the EU's *global* role in cyberspace conditioned the 2013 strategy's inward-facing orientation, which largely reproduced the territorial and political boundaries of the Internal Market. Furthermore, the debut *Cybersecurity Strategy: An Open, Safe, and Secure Cyberspace* emphasized the 'key challenge' of clarifying the 'roles and responsibilities of the many actors involved,' (p.17), suggesting that a coherent EU role in

and through cyberspace—a 'sense of Self'—remained elusive (see also Carrapico & Barrinha, 2017).

Nonetheless, the strategy was a significant moment of spatial (b)ordering for the Union by demarcating space for EU-level action in this domain. By envisioning an EU role within the bounds of the Internal Market, EU policymakers engaged familiar spatial (b)ordering routines (*routinization strategies)* to demarcate the EU's role in cyberspace. Underneath this umbrella, the strategy brought together several cyber-relevant policy issues discussed at the EU level (e.g. critical infrastructure, law enforcement) into a broader, pan-European strategic framework, and assigned specific roles to de novo EU agencies, including ENISA and the European Cybercrime Centre (p. 10). In terms of external action, the strategy further clarified the EEAS' role in cyberspace as *coordinating* a 'coherent' EU-wide strategy on international cybersecurity (European Commission and HRVP, 2013, p.17) and called for the mainstreaming of cyber issues into the EU's CFSP areas (pp. 13-15).

Altogether, during the 2009-2013 period, the question of borders loomed large in debates about the development of the EU's first cyber strategy. To manage the ontologically disruptive nature of cyberspace, EU policymakers constructed cyberspace within the bounds of the EU's Internal Market. In this way, EU institutions engaged familiar spatial (b)ordering routines to demarcate the EU's role in cyberspace and drew upon the Union's historical role as an economic security provider. This routinized approach to envisioning the boundaries of EU action in cyberspace laid the basic conceptual (and political) foundations for the Union's global role in later periods.

2014-2017: Ontological insecurity in and through cyberspace

Broadly, the 2014 Russian invasion of Ukraine, the 2015 migration crisis, the 2016 Brexit referendum and the 2016 election of American President Donald Trump constituted

significant ‘wake-up calls’ for European policymakers regarding the EU’s security environment (Interviewees A, C, D), stoking the impression that the Union was surrounded by a ‘ring of fire’ (European External Action Service, 2015, p.8). Thus, crises in the EU’s external Neighbourhood and rising anxieties about hybrid warfare (including in cyberspace) over the 2014-2017 period spurred a process of re-imagining the EU as a global (cyber) actor around a more externalised orientation. Notably, this process of external bordering and securitization in cyberspace also served to reinforce the existing boundaries of the European spatial imaginary of cyberspace laid out in the EU’s 2013 strategy.

After the Russian invasion of Ukrainian territory in 2014, the EU’s security environment had changed ‘dramatically’ (Interviewee D, European External Action Service, 2015, p. 8). Russian cyber operations crippled Ukrainian critical infrastructure and disseminated disinformation across the continent, leading to rising awareness across EU policy communities that cyberspace as a strategic domain had become increasingly unstable and unpredictable (Interviewee D). Hybrid cyber operations were therefore deemed hallmarks of the ‘changing global environment,’ demonstrating how cyberspace could serve as a site for geopolitically motivated, hybrid warfare (Interviewees A, C, D; M; Pawlak, 2015).

Significantly, these material security threats were also ontologically destabilizing for EU policymakers and the EU’s external action at large. Documentary and interview evidence suggests that these crises were understood by different EU actors as destabilizing for the EU’s self-conception as a global cyber actor and their ontology of cyberspace as a strategic environment. Multiple EU officials emphasized how it was difficult to ‘keep up’ with the evolving strategic context at this juncture, and they underscored the imperative for the EU to develop greater ‘situational awareness’ and to ‘build resilience’ against such an indeterminate threat (Interviewees A; D; K). Interviewees also lamented the lack of clear

rules and expectations for safe conduct in cyberspace (Interviewees A, B, D). For example, 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). Concerns about hybrid warfare, cyberespionage, disinformation, alongside several debilitating cyberattacks (i.e. WannaCry and NotPetya) during this period brought about the recognition that 'What's happening in cyber space is mirroring what's happening in the world (Interviewees D; K). As the EEAS stated 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 (emphasis added by author, p. 16).'

Accordingly, 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 (European Commission, 2015).

Meanwhile, the EU's sense of ontological security in global cyberspace may have been further destabilized by fraying transatlantic relations during this period. The EU's relationship with the United States (US) has historically played a key role in the EU's self-positioning as a global cyber and security actor (see also Flockhart, 2020). In fact, bilateral cooperation with Washington on digital and cyber issues has been the Union's oldest and arguably most important diplomatic arrangement in and through cyberspace (Interviewees I,K; Renard, 2018; Shahin, 2024). Thus, the EU's 2013 cyber strategy had positioned Washington as the EU's primary strategic partner in cyberspace, crucial for recognizing, supporting, and to an extent, *securing* the EU's role in global cyberspace. As then-Commission President Barroso affirmed, 'there is no more important partner than the United States [for the EU],' (2014, p. 23).

Whereas EU-US relations were marred by the 2013 ‘Snowden revelations’, they were further unsettled by President Donald Trump’s initial rise to office in 2016. As one interviewee explained, 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,’ (Interviewee C; see also European Parliament, 2016a). Altogether, the ontologically destabilizing context of these events, paired with the Union’s mounting sense of ‘existential crisis’ (Mogherini, 2016) suggests a significant disruption in the EU’s stable ‘sense of Self’ and ‘trust that the world is what it appears to be’ (Kinnvall 2004, p. 746; see also Malksöo, 2016). Indeed, 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 (Interviewee A, B, C, D, E).

Following these developments, the EU released its reconceptualized role in global affairs in the 2016 *Global Strategy* (EUGS). With the ‘aspiration to *transform* rather than simply preserve the existing system,’ (Mogherini, 2016; emphasis my own), the EUGS re-imagined the EU’s role in global cyberspace to become more strategic and ‘joined up’, laying out a vision for the EU to become a ‘*forward-looking cyber player*’ (2016, p. 42). The necessity of a ‘joined-up Union’ encompassed the greater incorporation of ‘all dimensions of EU external action, security and non-security related,’ (Barbé & Morrillas, 2019, p. 762). As a consequence of its new ‘joined-up approach’, the policy area of cybersecurity was taken under the wing of the EUGS framework (Barbé & Morrillas, 2019).

Significantly, beneath the EUGS’ ambitious vision to ‘help our Union to re-discover its identity, its soul,’ (Mogherini, 2016) was the mission of ‘keeping faith of the EU citizens in the continuous relevance of the Union,’ which sought to manage the EU’s insecurities

about the merits of a European approach to global affairs (Malksöo, 2016, p. 381). The ontological security imperatives for the 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. (European Union, 2016, p.2)'

Efforts to 'rethink' the EU's position in the world, as formalized by the EUGS, brought about an enthusiastic policy turn towards the external, relational, and spatial dimensions of cybersecurity (Interviewee A). For one, the strategy advanced a new, bolder discourse of European '*strategic autonom*y' (see for example pp. 45-46) achieved in cyberspace by engaging 'in cyber diplomacy and capacity building with our partners and seeking agreements on responsible state behaviour in cyberspace based on existing international law,' (p.42).

Furthermore, as a series of spatial (b)ordering moves, over a dozen EU cyber policy documents published between 2014-2017 constructed cybersecurity issues as 'cross border' or 'borderless' problems mandating EU-level intervention. In effect, this consolidated a European imaginary of cyberspace over a broad range of relevant and/or cyber-adjacent issues, including Russian disinformation (European Parliament, 2016b), cybercrime (European Parliament, 2017d), digital economy, trade, and the Digital Single Market (European Economic and Social Committee, 2015; European Parliament, 2017e; European Commission, 2016a,b, 2017a), data protection and flows (European Commission, 2017b), 5G networks and industrial strategy (European Parliament, 2017b), European cloud infrastructure (European Parliament, 2017a), and cybersecurity (European Commission,

2016c, 2017d; European Commission & High Representative of the European Union for Foreign Affairs and Security Policy, 2017; Council of the European Union, 2016).

In this contex, a second threat logic became prominent in EU cyber policy: the *externalization* of cyber threats (Interviewee K; (see for example European Commission & HRVP, 2017, pp. 14, 18, 19; see also European Commission, 2017c, p.7; see also Backman, 2023). Notably, emphasizing the rising importance of the EU's *external* role in global cyberspace constitutes a significant shift in the EU's self-representation from an inward-looking self-image towards an explicit and 'forward-looking' global outlook (see for example European Commission 2017, p. 20; European Parliament, 2017). Yet, at the same time, the securitization of the EU's external outside relied upon the European imaginary of cyberspace established in the 2013 strategy. These dual securitizing/externalising moves are illustrated by the EU's changed approach to cyber capacity building during this period.

Routinization and demarcation in the EU's cyber capacity building initiatives

After the 2014 Russian invasion of Ukraine, policymakers concluded that a greater focus should be placed upon the nexus between security and development in cyberspace (Carver, 2024b). Consequently, cyber capacity building programmes were reconceptualized from an emphasis on cybercrime to incorporate a stronger *cybersecurity* and geographically targeted orientation (Interviewee I; H). In fact, by 2015, cyber capacity building (CCB) was considered vital for the EU to achieve 'resilience' in its increasingly unstable global environment (European Parliament, 2016a; Interviewee A; European Union External Action Service, 2015, p. 5). In turn, the EUGS both formalized and accelerated the cross-dimensional approach to cybersecurity which had commenced after the Ukraine crisis.

To explain the remit of the EU's external CCB projects during this period, EU documents held that the 'borderless' nature of threats or malicious activities in cyberspace justified

further EU *external* intervention (Council of the European Union Presidency, 2016, p.5, emphasis my own; European Commission, 2018a, p. 3; see also Interviewee M). To manage such 'borderless' threats, CCB initiatives were adapted to reproduce the EU's logic of 'concentric circles' previously deployed to stabilize its (physical) Neighbourhood, which have used conditionality instruments to incentivize proximate partner countries to uptake EU norms and democratic mechanisms in line with European interests (see also Carver 2024a,b; Bialasiewicz, 2015; Browning, 2018; Freyburg & Richter, 2010).

Foregrounding the ontological security dimensions of this behaviour helps us to better understand why the 'borderless' nature of cyberspace *justified* the EU's externalising approach to EU cyber capacity building projects. Externalising cybersecurity threats in line with a familiar spatial logic can be understood as an ontological security management strategy, as the 2015-2018 programmes reproduced familiar spatialising routines practiced by other EU Neighbourhood policies (see also Browning, 2018).

These logics are exemplified by the EU's two flagship CCB initiatives during this period, CyberEAP and GLACY+, which were geographically targeted in the EU's Eastern and Southern Neigbourhoods to align with the EU's broader Neighbourhood approach. By exporting 'made in Europe' solutions, such as promoting the EU's *General Data Protection Regulation* (GDPR) and the EU-funded Budapest Convention on Cybercrime, these initiatives align with the EUGs' ontology of the global threat landscape: that is, 'our [EU] security at home depends upon peace beyond our borders,' (European Union, 2016, pp. 5-7). For example, the GDPR has been widely considered a form of EU 'extraterritorial' power projection in cyberspace (Kuner, 2019).

At the same time, these programmes can be understood as a spatial (b)ordering strategy to help manage the EU's ontological security, as they shape third countries' approaches to cybersecurity in line with the Union's own 'comforting' image (Interviewees A, O; see also

Browning, 2018; Mitzen, 2018). In fact, 'sharing' European approaches with third countries, including through conditionality instruments, have been perceived by EU policymakers as a way of alleviating the Union's dependency upon insecure others in cyberspace (Interviewee A, M, see also European Commission, 2018, p. 8). The notion of sharing the EU's success is similarly reproduced by official speeches, in the language of 'exporting Europe's stability' and the European model as 'inspiring others' (see for example Juncker, 2018). Overall, by 'familiarizing' or 'Europeanizing' the Union's 'external' cyberspace, these initiatives have sought to bring greater (geo)spatial order and security to the EU's position in cyberspace vis-à-vis others. By engaging with third countries with the aim of establishing stable expectations about safe conduct in cyberspace, projects such as the CyberEast Partnership (CyberEaP) programme have also responded to the EU's insecurities about its Neighbours in cyberspace, including mutual relations with Russia (see also Browning, 2018).

These practices illustrate how the EU's spatial (b)ordering moves in cyberspace during this period constituted a more securitized, external-facing EU role in cyberspace. More broadly, the EU's efforts to strengthen the Union's *external* action role (including in cyberspace) through a strategic, geographically targeted approach established the ideational and ontological precedents for the EU's future geostrategic self-narratives. Following the release of the *EUGS,* both EU publications and national debates across the Union evinced a greater openness towards approaching the EU's role through a power politics, geostrategic, and/or sovereigntist lens. For example, the Commission's *Reflection Paper on the Future of European Defence* conceived the EU as a '*continental-sized power*' (2016c, p.8), arguing that an enhanced role for the EU would strengthen Member States and make them 'more sovereign,' (p.11). Likewise, other EU documents cited '*geo-strategic*' reasons for a greater EU role (European Commission 2017, p. 20) and the critical importance of maintaining the

'EU's place in the world' (European Parliament, 2017c). Notably, the EU's updated cybersecurity strategy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* stressed the EU's objective to achieve 'greater resilience and strategic autonomy,' (p. 18) and emphasized the 'global dimension' to cybersecurity eleven times.

The EU's geostrategic ambitions were also supported by national discourses in France and Germany about the EU's role as a cybersecurity provider, in which there had already been 'lively and multilayered debate[s]' about the potential for 'digital sovereignty' in the European context (Interviewee C; Glasze et al., 2023, p. 929). These discourses provided more favourable conditions for EU actors to negotiate the development of a 'geostrategic Union' in the next time period.

2018-2024: Digital sovereignty, dependence, and geopolitics

Examining EU discourses and practices during the 2018-2024 period reveals further how the EU's geostrategic turn was not only shaped by material security pressures, but ontological security drives related to the Union's historical self-representation as a global actor. During this period, EU policymakers deployed various spatial (b)ordering moves to manage these insecurities, including geopolitical othering, Europeanization, and routinized narratives to 'locate' the EU's self in global cyberspace. Accordingly, EU actors' reliance upon routinized practices and geopolitical othering to construct the Union's adapted role as a geostrategic cyber actor underscores the significance of earlier spatial (b)ordering moves in cyberspace for conditioning the Union's contemporary behaviour.

Digital dependence anxieties and 'interdependence' as a weapon

The EU's geostrategic turn was not only characterized by the emergence of sovereigntist and geopolitical concepts (e.g. 'open strategic autonomy', the 'geopolitical Commission', and 'technological sovereignty') in EU discourse, but also by prevalent debates about

'digital dependence'. In fact, European 'strategic autonomy' was often framed as the solution to 'digital dependence' problems, a common theme in the EU's self-narrative as a 'geopolitical actor' (e.g. Draghi, 2024; Borrell, 2022; see also Carrapico & Farrand, 2024).

Issues relevant to 'digital dependence' and the need for 'European digital sovereignty' rose to the fore during transatlantic debates about the risks of Huawei 5G telecommunications infrastructure, a Chinese state-funded company which held a dominant market position across the Union (Interviewees B, K; see also Carver 2024b). Beyond intelligence and data sharing concerns, the economic and technological dominance of Chinese companies in the EU's 5G market raised worries in the EU about the lack of a level playing field in European industry (Interviewees A, E; Council of the European Union). Moroever, the Huawei debate inculcated the fear that Europe could become subject to the *(geo)political* motives of foreign state actors under conditions of digital dependence (Interviewees A, B, E; see also Monsees & Lambach, 2022). The geopolitical stakes of the Huawei debate were further clarified after European policymakers faced increasing 'pressure' from both the US and China to consider the Union's dependency on foreign actors for supplying and maintaining the bloc's critical digital infrastructure (Interviewees A, B, K).

In this context, the EU's reputation as a global partner and within NATO shaped the decision making of Member States, who were moved by the conviction that Europe's approach to 5G must not be perceived as solely a concession to Washington's demands for boycotting Huawei (Interviewee K). According to a senior EU Commission official, Member States

> 'wanted to do it for their own reasons and not just because the US were focusing on the issue…and therefore quite quickly, we came to the view, including the member states, that that meant an analysis of the market. And, without making a big a song and dance about it, that meant the Commission also had a contribution to make because we had the instruments to analyze the market (Interviewee K).'

Consequently, to respond to the 5G debate, the EU's response was legitimized in terms of internal market concerns anchored around the Union's *raison d'être* as a security actor.

Notably, the EU's self-narrative about the sanctity of the Single Market in this context (e.g. European Commission, 2019) established a basis for a 'greater [internal] acceptance' of the EU's (geo)strategic approach to cyberspace (Interviewee C; J; K). Thus, under the newly elected 'geopolitical Commission' in 2019, high level EU discourses constructed the Union's role as a more assertive geostrategic actor, reflecting its priorities to 'reinforc[e] the EU's role as a relevant international actor,' (Bassot, 2020; see also Csernatoni, 2022).

However, the outbreak of the COVID-19 pandemic introduced further *ontological insecurities* about the EU's agency as a global actor and its capacity to maintain its role as an economic security provider. As the EU (and the rest of the world) became more dependent on digital technologies for the necessities of life, including financial and physical wellbeing, policymakers perceived a heightened risk of reliance on foreign technologies for executing the EU's basic political functions, including fostering a 'European community' (Interviewees A, D, E). As the pandemic progressed, EU officials observed with increasing unease that cyber actors, including states, had 'weaponized interdependencies' in supply chains 'to get an edge in the [global geopolitical] competition,' (Interviewee E).

While extant scholarship has interrogated the material basis (and credibility) of weaponized interdependence as a strategic concept (see for example Drezner et al., 2021; Gjesvik, 2022), EU discourses post-COVID reveal how invoking the concept of weaponized interdependence expresses not only structural risks and material realities, but inherent beliefs about the future and their place within it. In fact, revelations about dependence during the pandemic were 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' (Borrell, in Weiler, 2020; see also Draghi, 2024). The destabilizing consequences of this realization for the EU's self-representation and ontology of global politics is revealed in a speech by High Representative Josep Borrell, where he admitted that,

> 'We believed that interdependency was a way of ensuring peace […] *And we had that in our DNA:* interdependency is a way of avoiding war. But today interdependency is a weapon. If you are dependent on me, I use this dependency in order to threaten you,' (Borrell, 2022).

Additionally, the widely discussed *Draghi report on European Competitiveness* (2024) laid bare European perceptions of dependence on the US and China, describing Europe as 'the most dependent' in a world 'undergoing dramatic change […] where some key economic dependencies are suddenly turning into geopolitical vulnerabilities' (Draghi, 2024, p. 1). When presenting his findings to the European Parliament, Mr. Draghi framed these conditions in existential, not only material security terms:

> 'The European Union exists to ensure that Europe's fundamental values are always upheld: democracy, freedom, peace, equity and prosperity in a sustainable environment. If Europe cannot any longer deliver these values for its people, *it will have lost its reason for being'* (Draghi, 2024, p. 2, emphasis my own).

Altogether, EU discourses have increasingly framed weaponized interdependence risks, including digital dependence, as infringing upon the EU's capacity act and fulfil its political *raison d'être.* For instance, the EU's recent recognition that 'interdependence is a weapon' creates tension between maintaining the EU's longstanding self-representation as a multilateral, cooperative actor on the one hand (in the words of Borrell, 'we had it in our DNA'), and Brussels' role as a (cyber)security provider and global technological leader on the other.

Below, I argue that the EU appears to have engaged in spatial (b)ordering practices, including European digital sovereigntist discourse, to manage its ontological insecurities exacerbated by anxieties about digital dependence. Notably, the EU's efforts to adapt to these

geostrategic objectives have partly relied upon precedents set by earlier spatial (b)ordering efforts in cyberspace. These dynamics are evidenced by the EU's 2020 cyber strategy.

Digital sovereignty, adaptation, and routinization in the 2020 EU cyber strategy

As a linchpin of the EU's geostrategic approach, the EU's 2020 *Cybersecurity Strategy for the Digital Decade* evinced the imperative for 'the EU [to] learn the language of power and act geopolitically' (Borrell, in Weiler, 2020) and it 'describe[d] how the EU can harness and strengthen all its tools and resources to be *technologically sovereign*,' (European Commission, 2024, emphasis my own). Reflecting the EU's geopolitical and sovereigntist objectives, the strategy advanced the goal of promoting an 'open global internet *with strong guardrails'* (p. 4, emphasis my own)—that is, the imperative for the EU to *strike a balance* between technological sovereignty and the need for international cooperation at the same time.

Seeking to balance the EU's competing aims of openness/cooperation and technological competitiveness/closure, the EU's updated 2020 cyber strategy has both adapted and reproduced the spatial precedents laid out in the 2013 and 2017 strategic documents. On the one hand, the EU's digital sovereignty approach constitutes a significant departure from the EU's 2013 strategy, which had concluded that 'centralised, European supervision is not the answer' (EUCS, p.17; see also Carrapico & Farrand, 2024). While 'sovereigntist' logics often underpin the foundational narratives of states, and their ontological security by extension (Krickel-Choi, 2022b), the EU's role as a sovereign in global cyberspace is relatively new, and it remains an emerging and contested concept within the EU context.[67] Indeed, the EU's digital sovereignty agenda (including in the 2020

[67]As I have argued elsewhere, broader notions of 'European sovereignty' became popularized at the EU level in 2017 in President Jean-Claude Juncker's *State of the Union* speech, which converged with notions of 'digital sovereignty' debated within some national and supranational contexts, before popular notions of 'European

strategy), demonstrates the EU's shift to a more centralized, authoritative, and ambitious European-level approach to cyberspace (see also Carrapico & Farrand, 2024). Therefore, in terms of the EU's 'technological sovereignty' objectives, EU's cyber strategy constitutes *spatial adaptation.*

Indeed, the EU's discourse of European digital sovereignty and/or technological sovereignty can be understood as a solution to both the EU's material security concerns and its related existential concerns. This is because 'European digital sovereignty' discourse ultimately conveys aspirations about the EU's collective 'capacity to act' in global affairs (Interviewee R; Council of the European Union, 2021; Bassot, 2020; European Commission, 2020a; Council of the European Union, 2021; see also Costa & Barbé, 2022). Concretely, Member States' support of the 'digital sovereignty' concept at the EU level was shaped by 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' (Interviewee A; see also Interviewees C, I, K, R). Accordingly, claiming sovereignty not only responds to the EU's material security concerns, but it may be responding to perceived weaknesses in the EU's capacity act in global affairs, as a way to (re)claim the Union's power and legitimacy in this context, and thereby reaffirm its legitimate role as a global leader and (economic) security provider for its constituents.

However, the EU's sovereigntist objectives have been characterized by contestation between EU policymakers and stakeholders surrounding the usage and meaning of sovereignty in EU policy discourse (Falkner et al., 2024; Juncos & Vanhoonacker, 2024; Franke & Varma, 2019). This suggests deep instabilities and uncertainties underlying the EU's (re)imagined role as a geopolitical and sovereign global actor, including in and through

---

digital sovereignty' rose to the fore in 2019 (Carver, 2024b). In this context, the emergence of sovereigntist concepts in EU cyber policy was partly shaped by concerns about weaponized interdependence, as described in the section above. See Chapter 5's section on 'discursive change' in the EU context for further reference.

cyberspace (Carver, 2024b; Haroche, 2023). Indeed, scholars have argued the EU's '*open* strategic autonomy' contains inherently contradictory objectives (Barrinha & Christou, 2022), therefore revealing policy incoherence (Broeders et al., 2023).

Significantly, the competing logics of 'openness' and 'strategic autonomy' may be reflective of the EU's efforts to establish a 'cognitive bridge' (Subotic, 2016) between the EU's past autobiographical narrative and its contemporary sovereigntist approach. This dynamic is suggested in the context of EU cybersecurity policy, wherein recent EU documents and policy elites have linked 'European digital sovereignty' discourse to the EU's historical role as a global leader, responsible player, and a champion of multilateralism. This discursive chain of association hearkens back to the EU's 2016 *Global Strategy,* which associated 'strategic autonomy' with the assertion that 'the EU will be guided by a strong sense of responsibility,' (p.8). This idea was later expressed by Commission President Juncker in his formal *State of the Union Speech*, who declared that 'it [was] time Europe took its destiny into its own hands' (p.5). The transposition of the EU's leadership role towards cyberspace was later reaffirmed by the 2017 *Reflection Paper on European Defence* (European Commission, 2017c)*,* together with the EU's 2017 cybersecurity strategy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (e.g. p.19), which emphasizes 'responsibility' in cyberspace and seeks to position the EU as an already established leader in the field.

In this way, the EU's cyber strategy also exemplifies *routinization*, as the text has reproduced existing narrative routines and geospatial practices in EU cyber policy. For example, by incorporating cyber capacity building instruments into the EU's wider geopolitical agenda, the strategy built upon the Europeanizing, geographically targeted bent of earlier external cyber capacity building initiatives from 2015-2017 (see also Carver, 2024a,b). Despite several policy changes to capacity building programmes, these initiatives

continue to promote partner countries' adherence to EU-approved global or European standards remains a priority for EU leadership (European Commission, 2022; see also Carver, 2024a). Notably, the EU's established position in global spatial order has been transposed to this context. For example, the Council 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,'* (2020, p. 13; see also Interviewee A; European Commission, 2020b).

More widely, both EU documents and key EU leaders have emphasized Europe's historical position as an economic and technological leader to justify the Union's current geoeconomic approach towards the internal market (see for example European Parliament and Council, 2021; European Parliament, 2019; European Commission, 2020b, p. 4, 7; 2010, p. 34; von der Leyen, 2019, 2019, p. 17; 2023; see also Monsees & Lambach, 2022). As demonstrated earlier, this self-narrative builds upon a decades-long routine in constructing an EU-level approach to cyberspace as maintaining the Union's *historically established* role as an economic security provider for European citizens (and Member States). Ten years earlier, the 2010 *Digital Agenda for Europe* underlined how '*Europe must continue* to play a leading role […] in promoting a governance of the internet as open and inclusive as possible' (p. 34; emphasis added my own).

In sum, these discourses can be understood as practices of *routinization,* which reaffirm the continuity between the EU's past role(s) as a global actor and its present behaviour. Such discourses reproduce earlier spatial (b)ordering moves deployed by EU actors to demarcate cyberspace in line with the Union's internal market and insecure external outside to the EU's contemporary geostrategic behaviour.

The EU's paradoxical global approach to cyberspace and ontological insecurity management behaviour

While the Union's geostrategic approach is intended to bolster its credibility as a strategic partner and empower the Union to be a 'relevant' international actor (Interviewee R; Borrell 2023; 2024), paradoxically, this positioning has also exacerbated EU policymakers' concerns about the Union's credibility as a partner. As suggested above, EU self-narratives about the Union's approach to global cyberspace have tended to conceive the EU as both a shrewd, geostrategic actor and a champion of the liberal international order (see for also Christou & Barrinha, 2022; Broeders et al., 2023). For example, the Council's 2022 *Conclusions* on *Digital Diplomacy* emphasized both the objectives of 'promot[ing] an open, free, global, stable and secure Internet based on the multi-stakeholder model of Internet governance,' (p. 3) *and* 'improv[ing] the EU's capability to monitor global digital regulatory activity, international data flows and the data privacy of EU citizens, patterns of digital trade, partnerships between third countries and their effects on the competition framework in the global market for digital technologies and services,' (p. 5; see also EEAS, 2020).

In terms of external action, my interview data suggests that the EU's digital sovereignty approach has elicited ontological insecurities about the EU's autobiographical coherence—and credibility—as a global partner. Multiple policymakers expressed frustration and anxiety about being misunderstood by third countries as endorsing a 'traditional' geopolitics and 'fortress Europe' approach—the very persona that the EU historically eschewed as a core pillar of its political existence (Interviewees A, E, R; see also Carver 2024b). Indeed, multiple EU officials independently voiced worries that European digital sovereignty could be 'misunderstood' as a guise for imperialism, colonialism, and/or 'traditional' geopolitics (Interviewees A, B, F, E). This is further suggested by scholarship which has established that EU policymakers have expressed insecurity and reluctance about

embodying the EU's geostrategic self-representation (Carver 2024b; see also Bauerle Danzmann & Meunier, 2024; see also Bradford, 2023; Haroche, 2023).

Accordingly, when discussing the EU's approach to cyber diplomacy, interviewees adopted the strategy of 'geopolitical othering' to distance the EU's approach from traditional geopolitics and 'fortress Europe' conceptions of sovereignty. This suggests that policymakers were attempting to manage ontological insecurities about the EU's self-representation as non/geopolitical. For example, when describing the EU's external approach to cyberspace, interviewees frequently contrasted the EU with 'traditional' (Westphalian) geopolitical actors: China, Russia, and the United States (Interviewees A, B, F, I). In so doing, the EU was described as *post-Westphalian* insofar as it lacked the trappings—and competences—of nation states in the area of security (Interviewees A, B, F). 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 (Interviewees A, C, R).

Similarly, interviewees portrayed EU-funded capacity building projects from the perspective of empowerment and co-ownership (Interviewees A, B, C, D, E), in which the EU does 'not present it [to countries]' as taking sides in 'geopolitical battles' (Interviewee E), and collectively stressed the EU's goals of providing a 'fair' and 'level playing field' for third countries (Interviewee A, D, E). As opposed to Russian and Chinese *asymmetric* digital development projects, officials stressed that the EU's approach has been guided by the principle of multilateralism, the multistakeholder model, and universal values, in which the EU and its third country partner 'co-own' the CCB project (Interviewee A, E, I). Altogether, interviewees' reliance upon 'geopolitical othering' suggests that the EU's previous a-geopolitical self-narrative has come into tension with the EU's new geostrategic ambitions, raising questions about the Union's credibility in the eyes of significant others.

These tensions reveal the importance of spatial (b)ordering for constructing the EU's global role in cyberspace. After all, engaging strategies of 'geopolitical othering' does not negate the underlying geostrategic dimension to these projects, nor their spatializing consequences. Rather, the power asymmetry in these cooperative agreements is glossed over or positively framed through geopolitical othering strategies. As one interviewee clarified with me: 'we don't want to have the blind followers [as in the case of China], we want to have conscious followers' (Interviewee A). Another interviewee acknowledged tensions in the EU's contemporary 'geopolitical' approach with its previous approach to internet governance, but they maintained that this new role was necessary for ensuring the Union's credibility in global strategic discussions, particularly with 'big players' such as the US and China (Interviewee R). In practice, the EU considers itself in competition with the US and China in the context of digital development and some aspects of cyber diplomacy (Carver, 2024a; see also Haroche, 2023). [68] Overall, the evidence suggests that EU grapples with a legitimacy dilemma related to its position on cooperative, global interdependence and asserting digital sovereignty claims, and underlying ontological insecurities related to the EU's contemporary geostrategic approach towards cyberspace.

Summary

This section revealed how spatial bordering practices have been leveraged by EU actors as ontological security strategies triggered by the evolving global environment, the EU's loss of trust in relations with other actors, and significant tensions in the EU's self-representation. In particular, the Union's first cyber strategy can be understood a broad spatial (b)ordering move towards a collective, Europeanized imaginary of cyberspace.

[68] While Brussels and Washington do not consider each other to be systemic geopolitical rivals, they compete over a variety of global digital policy issues, including data governance and cybersecurity best practices and norms. See also Carver 2024a.

However, soon after, the Union experienced a period of instability and ontological disruption, whereby material 'cross-border' threats were not only framed as physical security issues, but inherent to the EU's existence as a global political actor. The increasingly insecure global context during the 2014-2018 period, as well as the convergence between cybersecurity and core areas of EU competences (e.g. economic security and trade) raised both physical and ontological security concerns for EU institutions. These forces shaped the EU's explicit embrace of geostrategic logics from 2018-2024 and the autobiographical self-narratives it expressed to seek coherence between its previously a-geopolitical role with its new geostrategic approach. Overall, the EU's geostrategic role construction in cyberspace has been an ontologically fraught process shaped by ontological insecurities relevant to the EU's position in global cyberspace and various spatial (b)ordering moves. The wider implications of my findings are discussed below.

Discussion

While acknowledging the significance of material security concerns, this article sought to foreground the overlooked dimension of ontological security and its potential relationship to geostrategic behaviour in and through cyberspace. Drawing upon critical geopolitics and ontological security scholarship, I theorized that geostrategic behaviour in and through cyberspace may not only be conditioned by material security concerns, but also ontological security drives. Specifically, I argued that geostrategic behaviour can also manifest as spatial (b)ordering moves, which serve as strategies to manage an actor's ontological insecurities in and through cyberspace.

To probe the plausibility of my framework, I explored how an ontological security lens can help to explain the EU's puzzling geostrategic approach towards cyberspace. My empirical findings lend support to my theoretical framework by demonstrating that the EU's engagement with spatial (b)ordering moves is not only a reaction to systemic changes or

material security concerns, but ontological security drives. This is revealed by examining the constitutive and productive influence of spatial (b)ordering moves on the EU's development as a global cyber actor. Particularly, both the 2009-2013 and 2014-2017 periods, which predate the EU's explicitly geopolitical approach, evince efforts to 'border' European cyberspace. At the EU level, bordering practices first emerged as a discursive, inward-looking exercise—as an effort to break down internal barriers and set out a *European* cyberspace—which later translated into *externalising* bordering practices, as evidenced by the reorientation of the EU's cyber capacity building projects and the EU's wider externalising security logic. Finally, they are characterized by *geopoliticizing* bordering practices, characterized by a dual (internal/external) approach: internal spatial control and external power projection in and through cyberspace.

However, it must be emphasized that not all cybersecurity risks and threats are understood in existential terms, and they can be understood variably by actors within the same collective political organization (Backman & Stevens, 2024). Focusing upon the United Kingdom, Backman and Stevens underline the variety of 'risk logics' inherent to cybersecurity practices and find that most cybersecurity activities are 'normal and routine' (2024, p. 2441). To a more limited extent, this article revealed how cyber insecurities were perceived differently across EU institutions in terms of material or (existential) ontological security threats—or indeed both. Thus, I do not advance a normative claim that cybersecurity *should* be treated in existential terms, but I aim to foreground how ontological security seeking practices have provided opportunities for actors to engage in geostrategic behaviour--regardless of whether actors have 'wilfully or wrongly perceived [such issues] as existential' (Betz & Stevens, 2011, p. 74). Through this lens, I have demonstrated how the EU's geostrategic and sovereigntist behaviour has been intertwined with discourses of 'digital dependence' and existential cybersecurity concerns, which have offered the impetus

for the EU to engage in competitive, controlling, and authoritative practices in and through cyberspace.

Yet, as Backman and Stevens (2024) contend, cyber risk and security issues are more 'internally heterogeneous' than often presupposed by IR theory. Equally, the EU's understanding of cyber insecurities is not homogenous—rather it is subject to internal contestation and active deliberation at both horizontal and vertical policy levels. This study identified several areas of discursive contestation, including the construction of cybersecurity threats as 'cross-border' (and relevant to the EU policy) versus within the purview of national and/or international mandates, and the construction of the EU's role as a geopolitical and sovereigntist global cybersecurity actor. Elsewhere, Backman (2023) demonstrated how the EU's cyber strategies have shifted from an emphasis on 'risk-based' compared to 'threat-based' logics of cybersecurity—that is, a transition from a logic premised upon building resilience to systemic vulnerabilities to a logic focused upon defending against 'antagonists', 'external threats to referent objects' and direct causes of harm (p. 90).

This article has offered a limited view of 'normal and routine' cybersecurity activities, although this research suggests that cybersecurity routines could be conditioned by ontological security drives in certain contexts. Further research could explore this relationship; how various EU actors have engaged with different logics of risk pertinent to geostrategic competition, and how these conceptions of risk may trigger or reassure the EU's collective sense of ontological security. As Branch demonstrated in the case of the United States, the US military conjoined 'cyberspace' with the military 'domain' concept, 'allowed convincing parallels to be drawn to physical spaces' and to military and operational rationales (2017, p. 48). Similarly, key EU actors associated cyberspace with 'cross-border' risks and insecurities, linking cyberspace with familiar arguments for further European

integration, particularly in the context of economic security policy and international cooperation. In both examples, institutional actors deployed routinized spatial (b)ordering moves to manage the unsettling nature of cyberspace—by integrating the cyber environment and its constituent issues into familiar routines, imaginaries playbooks, and rationales.

By examining the ontological security dimension to the EU's geostrategic turn, this study has shed further light on a widely observed paradox in EU policy: the tension between the EU's ambitions as a geostrategic actor and its goals to promote an open, liberal international order (see for also Christou & Barrinha, 2022; Broeders et al., 2023). While the EU's 'open' and 'values-based' geostrategic approach appears to be a logical contradiction, an ontological security approach can help us to understand why the EU may have selectively retained aspects of its historical self-narrative ('open', 'responsible' and 'values-based') by tying these attributes to the Union's contemporary 'sovereigntist' approach. From an ontological security perspective, this discursive move seeks to bridge the gap between its a-geopolitical past and its contemporary geostrategic ambitions, thus mitigating autobiographical incoherence (see also Subotic, 2016).

Elsewhere, scholars have underscored how states can selectively activate dimensions of their historical self-narratives to create a 'cognitive bridge' between a foreign policy change and a familiar 'past' (Subotic, 2016). Examining the EU's development as a cyber actor therefore demonstrates that adopting geopolitical and sovereigntist frames may not only constitute familiar, *routine* behaviours, as scholars have typically emphasized (e.g. Eberle & Daniel, 2022; Guzzini, 2012, 2017), but they could also exemplify an actor's creative efforts to adapt their role to challenging environmental conditions. As Csernatoni argued elsewhere, the EU's evolving collective security imaginary has the 'double role of de-territorialising and de-centring certain national policy spaces' and in turn, to 're-cent[er]'

these spaces ‘as sites of legitimate hegemonic intervention for EU-level competence and governance,’ (2022, p. 397).

Furthermore, as I have illustrated in this paper, the EU’s ontological security drives can be understood to shape the Union’s quixotic self-narratives in the context of cyber diplomacy, including a rejection of ‘classical’ geopolitics whilst simultaneously claiming ‘learn the language of geopolitical power’ (Borrell, in Weiler, 2020). My empirical analysis illustrated how the EU’s ontological security drive to maintain a recognizable autobiographical narrative—whilst adapting to evolving material security threats—appears to have shaped EU actors’ engagement with ‘geopolitical othering’ and expression of ‘*European* digital sovereignty discourse’. In the context of cyber diplomacy, the EU’s approach to cyber diplomacy has been clarified as the opposite of invasive and *Westphalian* geopolitical intentions of other global cyber actors (particularly Russia and China) *and,* to a notable extent, from Washington’s approach to managing geopolitical competition in the digital domain (Christou & Barrinha, 2022; Carver, 2024a). At the same time, by advancing a distinctly *European* approach to ‘technological sovereignty’ and/or ‘digital sovereignty’, the Union has expressly differentiated itself from other global actors and advanced a legitimate claim to power over (European) cyberspace (see also Christou & Barrinha, 2022). From an ontological security perspective, these spatial (b)ordering moves differentiate the EU from significant others and therefore helps to secure the EU’s own Self in cyberspace. Accordingly, the EU’s ontological security drives may help to explain why the EU has advanced apparently contradictory geospatial/a-geopolitical logics towards cyberspace.

Conclusion

Overall, this article sought to offer several theoretical and empirical contributions to IR scholarship on geostrategic competition in and through cyberspace. Theoretically, the

paper introduced a novel theoretical framework for examining the potential ontological security dimension(s) to geostrategic behaviour in and through cyberspace. Empirically, my account offers an alternative approach to previous scholarship on the EU's geostrategic turn, which has concentrated upon material security concerns and structural variables as explananda.

By introducing further analytical tools to explore actors' engagement with geostrategic logics in and through cyberspace, this article contributes to IR literature on ontological security studies and scholarship in cybersecurity studies. For one, emphasizing routines as ontological security responses facilitates further dialogue with critical geopolitics scholarship on spatial (b)ordering moves (e.g. Branch, 2020; Lambach, 2024). In so doing, my findings also contribute to an emerging literature on the EU's 'geopolitical imaginary' in the digital age (e.g. Csernatoni, 2022; Monsees & Lambach, 2022). Further research could explore how, if at all, ontological security drives may have conditioned the EU's engagement with particular spatial (b)ordering moves in other areas of cybersecurity and external action, such as cyber defence. Additionally, scholars could explore how ontological security drives may condition the geostrategic behaviour of other cyber actors, such as the United Kingdom, the United States, and China, including with respect to their relations with the EU (see also Lai, 2023).

Ultimately, ontological security seeking practices help to anchor a foreign policy actor's sense of agency and identity, giving meaning to their strategic decision making and their relations with others (Subotic, 2016). In our increasingly uncertain, territorially complex, and 'weaponized' global environment (Flockhart, 2020), understanding how actors engage in self-affirming practices, including spatial (b)ordering moves, is crucial to make sense of geostrategic behaviour in the digital age.

Chapter 6 References

Agnew, J. A. (2004). *Geopolitics: Re-visioning World Politics*. United Kingdom: Routledge.

Agnew, J., Checkel, J. T., Deudney, D., & Mitzen, J. (2017). Symposium on Stefano Guzzini's (ed.) *The return of geopolitics in Europe? Social mechanisms and foreign policy identity crises* [Review of *The return of geopolitics in Europe? Social mechanisms and foreign policy identity crises*, by S. Guzzini]. *Cooperation and Conflict*, *52*(3), 399–422. https://www.jstor.org/stable/48512952

Ansip, A. (2007, May 2). Prime Minister Andrus Ansip's speech in Riigikogu. *Estonian Government Website.* https://www.valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu.

Bacchi, C. L., & Goodwin, S. (2016). *Poststructural policy analysis: A guide to practice.* Palgrave Macmillan.

Backman, S. (2023). Risk vs. threat-based cybersecurity: the case of the EU. *European Security,* 32(1), 85–103. https://doi.org/10.1080/09662839.2022.2069464

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, 1(2), 176–198. doi:10.1017/eis.2016.8

Baracani, E., & Kassim, H. (2024). The 'Geopolitical Commission': An end of term review. *JCMS: Journal of Common Market Studies, 62*(S1), 41–51. https://doi.org/10.1111/jcms.13673.

Barkawi, T. (2016). Decolonising war. *European Journal of International Security*, 1(2), 199–214. doi:10.1017/eis.2016.7.

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Barrinha, A., & Christou, G. (2022). Speaking sovereignty: the EU in the cyber domain. *European Security,* 31(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895

Barroso, J. M.D. (2012, September 12). *State of the Union 2012 address* [Speech]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_12_596.

Barroso, J. M. D. (2014). *European Commission 2004–2014: A testimony by the President with selected documents.* European Commission.

Bassot, É. (2020). *The von der Leyen Commission's priorities for 2019-2024* [European Parliament Briefing]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646148/EPRS_BRI(2020)646148_EN.pdf.

Bauerle Danzman, S., & Meunier, S. (2024). The EU's geoeconomic turn: From policy laggard to institutional innovator. *JCMS: Journal of Common Market Studies, 62*, 1097–1115. https://doi.org/10.1111/jcms.13599

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security, 31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, *44*(2), 147-164. https://doi.org/10.1177/0967010613478323

Betz, D., Stevens, T. (2017). *Cyberspace and the state: toward a strategy for cyber-power.* Routledge.

Bialasiewicz, L. (2015). *Europe in the world: EU geopolitics and the making of European spac*e. Routledge.

Blancato, F. G., & Carr, M. (2024). The trust deficit. EU bargaining for access and control over cloud infrastructures. Journal of European Public Policy, 1–32. https://doi.org/10.1080/13501763.2024.2441418.

Borrell, J. (2022, February 15). *CFSP and CSDP: Remarks by the High Representative/Vice-President Josep Borrell at the EP Plenary*. European Union External Action Service. https://www.eeas.europa.eu/eeas/cfsp-and-csdp-remarks-high-representativevice-president-josep-borrell-ep-plenary_en.

Borrell, J. (2024, September 26). *Op-ed by the High Representative/Vice-President Josep Borrell: The Draghi report and Europe's geopolitical future*. European External Action Service. https://www.eeas.europa.eu/eeas/op-ed-high-representativevice-president-josep-borrell-draghi-report-and-europes-geopolitical-future_en.

Bradford, A. (2023). Digital empires: The global battle to regulate technology. Oxford University Press.

Branch, J. (2017). Territory as an institution: Spatial ideas, practices and technologies. *Territory, Politics, Governance, 5*(2), 131-144. https://doi.org/10.1080/21622671.2016.1265464.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization, 75*(1), 39–70. doi:10.1017/S002081832000051X.

Branch, J. (2024). Territory, sovereignty, and boundaries in digital battlespace. In T. Stevens & J. Devanny (Eds.), In *Research Handbook on Cyberwarfare* (pp. 301–315). Cheltenham, UK: Edward Elgar Publishing.

Broeders, D., Adamson, L., & Creemers, R. (2019). Coalition of the unwilling? Chinese and Russian perspectives on cyberspace. *The Hague Program for Cyber Norms Policy Brief*. SSRN. https://ssrn.com/abstract=3493600.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and

strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, 61, 1261–1280. https://doi.org/10.1111/jcms.13462.

Browning, C. S. (2018). Geostrategies, geopolitics and ontological security in the Eastern neighbourhood: The European Union and the 'new Cold War'. *Political Geography, 62*, 106-115. https://doi.org/10.1016/j.polgeo.2017.10.009.

Browning, C. S., & Christou, G. (2010). The constitutive power of outsiders: The European Neighbourhood Policy and the Eastern Dimension. *Political Geography, 29*, 109–118. https://doi.org/10.1016/j.polgeo.2010.02.009.

Browning, C. S., & Joenniemi, P. (2017). Ontological security, self-articulation and the securitization of identity. *Cooperation and Conflict, 52*(1), 31–47. https://doi.org/10.1177/0010836716653161.

Buchanan, B. (2020). *The hacker and the state : cyber attacks and the new normal of geopolitics.* Harvard University Press.

Bull, H. (1982). Civilian power Europe: A contradiction in terms? *Journal of Common Market Studies, 21*(2), 149–164. https://doi.org/10.1111/j.1468-5965.1982.tb00866.x

Cabinet Office. (2009). Memorandum by Department of Business, Innovation and Skills, Office of Cyber Security. *European Union Committee*. https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/9110402.htm.

Cadier, D. (2019). The Geopoliticisation of the EU's Eastern Partnership. *Geopolitics*, 24(1), 71–99. https://doi.org/10.1080/14650045.2018.1477754

Cai, C. (2018). Geopolitics in the cyberspace: A new perspective on U.S.-China relations. *The Journal of International Studies, 39*(1). Retrieved from http://jtp.cnki.net/bilingual/detail/html/GJZY201801001?view=3

Car, P. (2024). Cybersecurity actors in the EU. *European Parliamentary Research Service.* https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757594/EPRS_ATA(2024)757594_EN.pdf.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber)security actor? *Journal of Common Market Studies, 55*(6), 1254–1272. https://doi.org/10.1111/jcms.12575.

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *JCMS: Journal of Common Market Studies, 62*(1), 147–158. https://doi.org/10.1111/jcms.13654.

Carver, J. (2024a). Developing digital "peripheries" for strategic advantage: Capacity building assistance and strategic competition in Africa. *Contemporary Security Policy,* 1–42. https://doi.org/10.1080/13523260.2024.2430021.

Carver, J. (2024b). More bark than bite? European digital sovereignty discourse and changes

to the European Union's external relations policy. *Journal of European Public Policy,* 31(8), 2250–2286. https://doi.org/10.1080/13501763.2023.2295523.

Cash, J. (2016). To dwell in ambivalence: On the promise and dilemmas of Beck's The Art of Doubt. In E. L. Hsu & A. Elliott (Eds.), *The consequences of global disasters* (1st ed., pp. 169–181). Routledge. https://doi.org/10.4324/9781315716060-15.

Chander, A., & Sun, H. (2021). Sovereignty 2.0. *Georgetown Law Faculty Publications and Other Works*, 2404. https://scholarship.law.georgetown.edu/facpub/2404.

Christou, A., & Damro, C. (2024). Frames and issue linkage: EU trade policy in the geoeconomic turn. *JCMS: Journal of Common Market Studies, 62,* 1080–1096. https://doi.org/10.1111/jcms.13598.

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy.* Palgrave Macmillan.

Clark, J., & Jones, A. (2011). The spatialising politics of European political practice: Transacting 'eastness' in the European Union. *Environment and Planning: Society and Space, 29*(2), 291–308. https://doi.org/10.1068/d4609.

Cohen, J. E. (2007). *Cyberspace as/and space. Georgetown Law Faculty Publications and Other Works,* 807. https://scholarship.law.georgetown.edu/facpub/807

Council of the European Union. (2016, November 15). *Council conclusions on strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry* (ST-14540-2016-INIT).

Council of the European Union. (2021, February 3). *Digital sovereignty is central t European strategic autonomy – Speech by President Charles Michel at 'Masters of Digital 2021' online event*. https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/.

Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European Security,* 31(3), 395–414. https://doi.org/10.1080/09662839.2022.2103370.

Damro, C. (2012). Market power Europe. *Journal of European Public Policy, 19*(5), 682–699. doi:10.1080/13501763.2011.646779.

Della Sala, V. (2017). Homeland security: territorial myths and ontological security in the European Union. *Journal of European Integration, 39*(5), 545–558. https://doi.org/10.1080/07036337.2017.1327528.

Diez, T. (2004). Europe's others and the return of geopolitics. *Cambridge Review of International Affairs, 17*(2), 319–335. https://doi.org/10.1080/0955757042000245924.

Douzet, F. (2014). Understanding cyberspace with geopolitics. Hérodote, 1(152–153), 3–21.

https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm.

Draghi, M. (2024, September 17). Address by Mr. Draghi – Presentation of the report on the future of European competitiveness. European Commission. https://commission.europa.eu/document/download/fcbc7ada-213b-4679-83f7-69a4c2127a25_en?filename=Address%20by%20Mario%20Draghi%20at%20the%20Presentation%20of%20the%20report%20on%20the%20future%20of%20European%20competitiveness.pdf.

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making:
the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy,* 30(7), 1330–1352. https://doi.org/10.1080/13501763.2023.2173274.

Dunn Cavelty, M., & Wenger, A. (Eds.). (2022). *Cyber security politics: Socio-technological transformations and political fragmentation*. Routledge.

Eberle, J., & Daniel, J. (2022). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics,
and the Janus-faced politics of anxiety. *Political Geography, 92*, 102502. https://doi.org/10.1016/j.polgeo.2021.102502.

EOS ICT / Cyber-Security Working Group. (2011). *Steps towards implementing a European cyber-security strategy.* European Organization for Security. https://www.eos-eu.com/Files/Cuber-policy-docs/EOS_2011_11_CyberSec%20White%20Paper_final.pdf.

Eurobarometer. (2010). *European Commission Eurobarometer 74 Autumn 2010: Information on European political matters report.* European Commission. http://ec.europa.eu/public_opinion/index_en.htm.

European Commission. (2009). *Communication - "Protecting Europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience" [COM/2009/0149 final].*

European Commission. (2010). *A Digital Agenda for Europe* [COM/2010/245 final].

European Commission. (2011a, April 18). *Evaluation report on the Data Retention Directive [COM/2011/225 final].*

European Commission. (2011b, June 16). *Data protection: Europeans share data online, but privacy concerns remain – new survey* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_11_742.

European Commission. (2013a). *Eurobarometer survey on internal security: The economic crisis and terrorism top the agenda; Special Eurobarometer 404: Cyber security*. http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf.

European Commission. (2013b). *Proposal for a directive of the European Parliament and*

of the Council concerning measures to ensure a high common level of network and information security across the Union [COM/2013/048 final - 2013/0027].

European Commission. (2015). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions: The European Agenda on Security* [COM/2015/0185 final].

European Commission. (2016a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — EU eGovernment Action Plan 2016-2020: Accelerating the digital transformation of government* [COM/2016/179 final].

European Commission. (2016b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions — ICT standardisation priorities for the Digital Single Market* [COM/2016/176 final].

European Commission. (2016c). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* [COM/2016/410 final].

European Commission. (2017a). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All* [COM/2017/228 final].

European Commission. (2017b). *Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union* [SWD/2017/304 final].

European Commission. (2017c). *Reflection paper on the future of European defence*. https://www.eeas.europa.eu/sites/default/files/reflection-paper-defence_en_1_0.pdf.

European Commission. (2017d). *Report from the Commission to the European Parliament and the Council on the evaluation of the European Union Agency for Network and Information Security (ENISA)* [COM/2017/0478 final].

European Commission. (2018a). *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*.

European Commission. (2018b). *Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial,*

Technology and Research Competence Centre and the Network of National Coordination Centres [SWD/2018/403 final/2].

European Commission. (2019). *Communication from the Commission to the European Parliament, the European Council and the Council: Twentieth progress report towards an effective and genuine security union [COM/2019/552 final]*.

European Commission. (2020a). *2020 Strategic Foresight Report: Charting the course towards a more resilient Europe* [COM/2020/493 final].

European Commission. (2020b). *Shaping Europe's Digital Future*. https://commission.europa.eu/document/download/84c05739-547a-4b86-9564-76e834dc7a49_en?filename=communication-shaping-europes-digital-future-feb2020_en.pdf.

European Commission. (2022). *New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661.

European Commission. (2024, September 24). *The Cybersecurity Strategy*. [Web]. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy.

European External Action Service. (2015). *Food-for-thought paper 'Countering hybrid threats'. Retrieved from* http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf.

European External Action Service. (2016). *Shared vision, common action: A stronger Europe – A global strategy for the European Union's foreign and security policy*. https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf.

European External Action Service. (2020, September 14). Cyber diplomacy and shifting geopolitical landscapes. European Union. https://www.eeas.europa.eu/eeas/cyber-diplomacy-and-shifting-geopolitical-landscapes_und.

European External Action Service. (2021). *Military vision and strategy for cyberspace*. Retrieved from https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf.

European Commission & High Representative of the European Union for Foreign Affairs and Security Policy. (2013). *Cybersecurity strategy of the European Union: An open, safe, and secure cyberspace* [JOIN/2013/1 final].

European Commission & High Representative of the European Union for Foreign Affairs and Security Policy. (2017). *Joint communication to the European Parliament and the Council: Resilience, deterrence and defence: Building strong cybersecurity for the EU* [JOIN/2017/0450 final].

European Commission & High Representative of the European Union for Foreign Affairs

and Security Policy. (2020). *Joint communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade [JOIN/2020/18 final]*.

European Economic and Social Committee. (2015). *Opinion on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions — A Digital Single Market Strategy for Europe'* [COM/2015/192 final].

European Organisation for Security. (2011). *Towards a concerted EU approach to cyber security.* EOS ICT / Cyber-Security Working Group. https://www.eos-eu.com/Files/Cuber-policy-docs/EOS_2011_11_CyberSec%20White%20Paper_final.pdf

European Parliament. (2007). *European Parliament resolution of 24 May 2007 on Estonia* [P6_TA(2007)0215].

European Parliament. (2010). *European Parliament resolution of 15 June 2010 on internet governance: The next steps* [2009/2229(INI), P7_TA(2010)0208].

European Parliament. (2012). *European Parliament resolution of 22 November 2012 on cyber security and defence [2012/2096(INI)].*

European Parliament. (2013). *European Parliament resolution of 12 September 2013 on a cybersecurity strategy of the European Union: An open, safe, and secure cyberspace [2013/2606(RSP)].*

European Parliament. (2016a). *Resolution of 13 April 2016 on the EU in a changing global environment – a more connected, contested and complex world* [2015/2272(INI)].

European Parliament. (2016b). *Resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties* [2016/2030(INI)].

European Parliament. (2017a). *Resolution of 16 February 2017 on the European Cloud Initiative* [2016/2145(INI)].

European Parliament. (2017b). *Resolution of 1 June 2017 on internet connectivity for growth, competitiveness and cohesion: European gigabit society and 5G* [2016/2305(INI)].

European Parliament. (2017c). *Resolution of 15 June 2017 on online platforms and the digital single market* [2016/2276(INI)].

European Parliament. (2017d). *Resolution of 3 October 2017 on the fight against cybercrime* [2017/2068(INI)].

European Parliament. (2017e). *Resolution of 12 December 2017 on 'Towards a digital trade strategy'* [2017/2065(INI)].

European Parliament. (2019). *European Parliament resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them [2019/2575(RSP)]*.

European Parliament. (2023, June 26). *What think tanks are thinking*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/749803/EPRS_BRI(2023)749803_EN.pdf.

European Union Committee. (2010). *5th Report of Session 2009–10: Protecting Europe against large-scale cyber-attacks: Report with evidence.* House of Lords, United Kingdom. https://publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf.

Fahey, E. (2024). The evolution of EU–US cybersecurity law and policy: on drivers of convergence. *Journal of European Integration, 46*(7), 1073–1088. https://doi.org/10.1080/07036337.2024.2411240.

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy, and sovereignty. *International Affairs, 100*(6), 2379–2397. https://doi.org/10.1093/ia/iiaa156.

Fassi, E., Ceccorulli, M., & Lucarelli, S. (2023). An illiberal power? EU bordering practices and the liberal international order. *International Affairs, 99*(6), 2261–2279. https://doi.org/10.1093/ia/iiad228.

Fischerkeller, M. P., Goldman, E. O., & Harknett, R. J. (2022). *Cyber persistence theory: Redefining national security in cyberspace*. Oxford University Press.

Fisher Onar, N., & Nicolaïdis, K. (2013). The decentring agenda: Europe as a post-colonial power. *Cooperation and Conflict, 48*(2), 283–303. https://doi.org/10.1177/0010836713485384.

Flockhart, T. (2016). The problem of change in constructivist theory: Ontological security seeking and agent motivation. *Review of International Studies, 42*(5), 799–820. doi:10.1017/S026021051600019X.

Flockhart, T. (2020). Is this the end? Resilience, ontological security, and the crisis of the liberal international order. *Contemporary Security Policy, 41*(2), 215–240. https://doi.org/10.1080/13523260.2020.1723966.

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: towards digital sovereignty. *Journal of European Public Policy*, *31*(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179.

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy, 45(*3), 426–458. https://doi.org/10.1080/13523260.2024.2365062.

Franke, U., & Varma, T. (2019). Independence play: Europe's pursuit of strategic autonomy.

European Council on Foreign Relations. https://ecfr.eu/wp-content/uploads/Independence-play-Europes-pursuit-of-strategic-autonomy.pdf.

Freyburg, T., & Richter, S. (2010). National identity matters: The limited impact of EU political conditionality in the Western Balkans. *Journal of European Public Policy, 17*(2), 263–281. https://doi.org/10.1080/13501760903561450.

Gartzke, E., & Lindsay, J. R. (2015). Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies, 24*(2), 316–348. https://doi.org/10.1080/09636412.2015.1038188.

General Secretariat of the Council of the EU & EU Institute for Security Studies. (2009). Seminar on cyber security: What role for CFSP? Organised jointly by the General Secretariat of the Council of the EU & the EU Institute for Security Studies in cooperation with Estonia, held in Brussels on 4 February 2009.

General Secretariat of the Council. (2021). *Draft Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade [6722/21]*.

Gjesvik, L. (2022). Private infrastructure in weaponized interdependence. *Review of International Political Economy, 30*(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics,* 28(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070.

Gomez, M. A., & Whyte, C. (2021). Breaking the myth of cyber doom: Securitization and normalization of novel threats. *International Studies Quarterly, 65(*4), 1137–1150. https://doi.org/10.1093/isq/sqab034.

Gstöhl, S., & Schunz, S. (2023). Governing Global Spaces: the roles of the European Union and other major powers. *Journal of European Integration, 45*(8), 1235–1254. https://doi.org/10.1080/07036337.2023.2270616.

Guzzini, S. (2012). *The return of geopolitics in Europe? Social mechanisms and foreign policy identity crises.* Cambridge University Press. https://doi.org/10.1017/CBO9781139225809.

Guzzini, S. (2017). Militarizing politics, essentializing identities: Interpretivist process tracing and the power of geopolitics. *Cooperation and Conflict, 52*(3), 423-445. https://doi.org/10.1177/0010836717719735.

Hagström, L. (2021). Great power narcissism and ontological (in)security: The narrative mediation of greatness and weakness in international politics. *International Studies Quarterly, 65*(2), 331–342. https://doi.org/10.1093/isq/sqab011.

Hansen, L. (2006). *Security as practice: Discourse analysis and the Bosnian war.* Routledge.

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

Haroche, P. (2023). A 'Geopolitical Commission': Supranationalism meets global power competition. *JCMS: Journal of Common Market Studies, 61*(4), 970–987. https://doi.org/10.1111/jcms.13440.

Heidebrecht, S. (2024). From market liberalism to public intervention: Digital sovereignty and changing European Union digital single market governance. *JCMS: Journal of Common Market Studies, 62*, 205–223. https://doi.org/10.1111/jcms.13488.

Herranz-Surrallés, A., Damro, C., & Eckert, S. (2024). The geoeconomic turn of the Single European Market? Conceptual challenges and empirical trends. *JCMS: Journal of Common Market Studies, 62*(1), 159–171. https://doi.org/10.1111/jcms.13591.

Home Office. (2010). *Protecting Europe against large-scale cyber-attacks: The government reply to the fifth report from the House of Lords European Union Committee, Session 2009-10, HL Paper 68*. United Kingdom. Retrieved from https://www.parliament.uk/globalassets/documents/lords-committees/eu-sub-com-f/govttresponsefinal060710.pdf.

House of Commons European Committee B. (2013-2014). *EU strategy for an open, safe, and secure cyberspace* [General Committee Debate]. https://publications.parliament.uk/pa/cm201314/cmgeneral/euro/130708/130708s01.htm.

House of Lords, European Union Committee. (2011). *17th Report of Session 2010–12: The EU internal security strategy.* House of Lords Publications. Retrieved from https://www.statewatch.org/media/documents/news/2011/may/eu-internal-security-uk-hol-report.pdf

Juncker, J. C. (2018). *State of the Union 2018: The hour of European sovereignty*. European Commission. https://commission.europa.eu/system/files/2018-09/soteu2018-speech_en_0.pdf.

Juncos, A. E. (2017). Resilience as the new EU foreign policy paradigm: A pragmatist turn? *European Security, 26*(1), 1–18. https://doi.org/10.1080/09662839.2016.1247809.

Juncos, A. E., & Vanhoonacker, S. (2024). The ideational power of strategic autonomy in EU security and external economic policies. JCMS: Journal of Common Market Studies, 62(4), 955–972. https://doi.org/10.1111/jcms.13597.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kinnvall, C. (2004). Globalization and Religious Nationalism: Self, Identity, and the Search for Ontological Security. *Political Psychology 25*(5): 741-767, https://doi.org/10.1111/j.1467-9221.2004.00396.x.

Klimburg, A., & Tirmaa-Klaar, H. (2011). *Cybersecurity and cyberpower: Concepts, conditions, and capabilities for cooperation for action within the EU*. Directorate-General for External Policies of the Union, Directorate B, Policy Department. https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf.

Klose, S. (2018). Theorizing the EU's actorness: Towards an interactionist role theory framework. *JCMS: Journal of Common Market Studies, 56*, 1144–1160. https://doi.org/10.1111/jcms.12725.

Klose, S. (2020). Interactionist role theory meets ontological security studies: an exploration of synergies between socio-psychological approaches to the study of international relations. *European Journal of International Relations,* 26(3), 851-874. https://doi.org/10.1177/1354066119889401.

Klose, S. (2023). Does the EU have friends? *JCMS: Journal of Common Market Studies*, 61(3), 579–596. https://doi.org/10.1111/jcms.13401.

Krickel-Choi, N. C. (2021). The embodied state: Why and how physical security matters for ontological security. *Journal of International Relations and Development*, 25(1), 159–181. https://doi.org/10.1057/s41268-021-00219-x.

Krickel-Choi, N. C. (2022a). The concept of anxiety in ontological security studies. *International Studies Review,* 24(3), viac013. https://doi.org/10.1093/isr/viac013.

Krickel-Choi, N. C. (2022b). State personhood and ontological security as a framework of existence: moving beyond identity, discovering sovereignty. *Cambridge Review of International Affairs*, 37(1), 3–21. https://doi.org/10.1080/09557571.2022.2108761.

Kuner, C. (2019). The internet and the global reach of EU law. In M. Cremona & J. Scott (Eds.), *EU law beyond EU borders: The extraterritorial reach of EU law* (pp. 112–145). Oxford University Press.

Kurowska, X., & de Guevara, B. (2020). Interpretive approaches in political science and international relations. In L. Curini & R. Franzese (Eds.), *The SAGE Handbook of Research Methods in Political Science and International Relations* (pp. 1211–1230). SAGE Publications Ltd.

Lai, S., Bacon, P., & Holland, M. (2023). Three decades on: Still a capability–expectations gap? Pragmatic expectations towards the EU from Asia in 2020. *JCMS: Journal of Common Market Studies, 61*(3), 451–468. https://doi.org/10.1111/jcms.13382.

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review*, *22*(3), 482–506. https://doi.org/10.1093/isr/viz022.

Lambach, D. (2024). B/ordering the state in cyberspace. In A. Fellner, K. Jungbluth, H. Krämer, & C. Wille (Eds.), *Border studies: Cultures, spaces, orders* (pp. 285-307). Europa-Universität Viadrina Frankfurt.

Laine, J. P. (2020). Ambiguous bordering practices at the EU's edges. In A. Bissonnette &

É. Vallet (Eds.), *Borders and border walls: In-security, symbolism, vulnerabilities* (pp.69-87). Routledge.

Liebetrau, T. (2024). Problematising EU cybersecurity: Exploring how the single market functions as a security practice. *JCMS: Journal of Common Market Studies, 62*(3), 705–724. https://doi.org/10.1111/jcms.13523

Liebetrau, T., & Christensen, K. K. (2021). The ontological politics of cybersecurity: Emerging agencies, actors, sites, and spaces. *European Journal of International Security, 6*(1), 25–43. https://doi.org/10.1017/eis.2020.10

Lindsay, J. R., & Gartzke, E. (2020). Politics by many other means: The comparative strategic advantages of operational domains. *Journal of Strategic Studies*, 45(2), 746. https://doi.org/10.1080/01402390.2020.1768372.

Lonergan, E. D., & Schneider, J. (2023). The power of beliefs in US cyber strategy: The evolving role of deterrence, norms, and escalation. *Journal of Cybersecurity*, *9*(1), 1-10.

Lupovici A (2016) *The Power of Deterrence: Emotions, Identity and American and Israeli Wars of Resolve.* Cambridge: Cambridge University Press.

Lupovici, A. (2023). Ontological security, cyber technology, and states' responses. *European Journal of International Relations, 29*(1), 153-178. https://doi.org/10.1177/13540661221130958.

Mälksoo, M. (2016). From the ESS to the EU Global Strategy: external policy, internal purpose. *Contemporary Security Policy, 37*(3), 374–388. https://doi.org/10.1080/13523260.2016.1238245.

Manners, I. (2002). Normative power Europe: A contradiction in terms? *JCMS: Journal of Common Market Studies*, 40(2), 235–258. https://doi.org/10.1111/1468-5965.00353

Maschmeyer, L. (2023). Subversion, cyber operations, and reverse structural power in world politics. *European Journal of International Relations*, *29*(1), 79–103. doi:10.1177/13540661221117051.

McCarthy, D. R. (2015). *Power, information technology, and international relations theory: The power and politics of US foreign policy and the internet*. London: Palgrave Macmillan.

McDermott, R. (2019). Some emotional considerations in cyber conflict. *Journal of Cyber Policy, 4*(3), 309–325. https://doi.org/10.1080/23738871.2019.1701692.

McNamara, K. R. (2023). Transforming Europe? The EU's industrial policy and geopolitical turn. Journal of European Public Policy, 31(9), 2371–2396. https://doi.org/10.1080/13501763.2023.2230247.

Mills, R. E. (2014). The pirate and the sovereign: Negative identification and the constitutive

rhetoric of the nation-state. *Rhetoric and Public Affairs, 17*(1), 105–136. https://doi.org/10.14321/rhetpublaffa.17.1.0105.

Mitzen, J. (2018a). Anxious community: EU as (in)security community. *European Security, 27*(3), 393–413. https://doi.org/10.1080/09662839.2018.1497985

Mitzen, J. (2018b). Feeling at Home in Europe: Migration, Ontological Security, and the Political Psychology of EU Bordering. *Political Psychology, 39*(6), 1373–1387. http://www.jstor.org/stable/45095213.

Moisio, S., & Paasi, A. (2013). Beyond State-Centricity: Geopolitics of Changing State Spaces. *Geopolitics,* 18(2), 255–266. https://doi.org/10.1080/14650045.2012.738729.

Möllers, N. (2021). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, *46*(1), 112-138. https://doi.org/10.1177/0162243920904436.

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security, 31*(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883.

Moravcsik, A. (1998). *The choice for Europe: Social purpose and state power from Messina to Maastricht*. Routledge.

Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace* (4th ed.). New York, NY: Alfred A. Knopf.

Mueller, M. (2020). Against sovereignty in cyberspace. *International Studies Review, 22*(4), 779–801. https://doi.org/10.1093/isr/viaa030

Mügge, D. (2024). EU AI sovereignty: for whom, to what end, and to whose benefit? Journal of European Public Policy, 31(8), 2200–2225. https://doi.org/10.1080/13501763.2024.2318475.

Neumann, I. B. (1998). European Identity, EU Expansion, and the Integration/Exclusion Nexus. *Alternatives,* 23(3), 397-416. https://doi.org/10.1177/030437549802300305.

Ó Tuathail, G. (1998). Postmodern geopolitics? The modern geopolitical imagination and beyond. In S. Dalby & G. Ó Tuathail (Eds.), Rethinking geopolitics (1st ed., pp. 16–38). Routledge. https://doi.org/10.4324/9780203058053.

Paasi, A. (2022). Examining the persistence of bounded spaces: Remarks on regions, territories, and the practices of bordering. *Geografiska Annaler: Series B, Human Geography, 104*(1), 9–26. https://doi.org/10.1080/04353684.2021.2023320.

Pamment, J., Sazonov, V., Granelli, F., Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Gravelines, J.-P., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Sari, A., Simons, G., & Terra, J. (2019). *Hybrid threats: 2007 cyber attacks on Estonia.* NATO Strategic Communications

Centre of Excellence. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Radu, R. (2023). DNS4EU: a step change in the EU's strategic autonomy? *Journal of Cyber Policy, 8*(2), 239–256. https://doi.org/10.1080/23738871.2023.2295937

Renard, T. (2018). EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, 19(3), 321–337. https://doi.org/10.1080/23745118.2018.1430720.

Sassen, S. (2015). From national borders to embedded borderings: One angle into the question of territory and space in a global age. In W. de Been, P. Arora, & M. Hildebrandt (Eds.), *Crossroads in new media, identity and law* (pp. 19-33). Palgrave Macmillan. https://doi.org/10.1057/9781137491268_2.

Schimmelfennig, F. (2021). Rebordering Europe: external boundaries and integration in the European Union. *Journal of European Public Policy, 28*(3), 311–330. https://doi.org/10.1080/13501763.2021.1881589.

Schindler, S., Alami, I., DiCarlo, J., Jepson, N., Rolf, S., Bayırbağ, M. K., … Zhao, Y. (2023). The Second Cold War: US-China Competition for Centrality in Infrastructure, Digital, Production, and Finance Networks. *Geopolitics, 29*(4), 1083–1120. https://doi.org/10.1080/14650045.2023.2253432.

Shahin, J. (2024). Dancing to the same tune? EU and US approaches to standards setting in the global digital sector. *Journal of European Integration, 46*(7), 1111–1131. https://doi.org/10.1080/07036337.2024.2398430.

Simmons, B. A., & Hulvey, R. A. (2023). *Cyberborders: Managing interdependence in the information age*. *Faculty Scholarship at Penn Carey Law*, 3158. https://scholarship.law.upenn.edu/faculty_scholarship/3158.

Slayton, R. (2016). What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security,* 41(3), 72–109. https://www.jstor.org/stable/26777791.

Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy, 35*(3), 468–486. https://doi.org/10.1080/13523260.2014.959261.

Smith, H. (2023). The geopolitics of cyberspace and the European Union's changing identity. *Journal of European Integration*, 45(8), 1219–1234. https://doi.org/10.1080/07036337.2023.2277329.

Soifer, H., & vom Hau, M. (2008). Unpacking the strength of the state: The utility of state infrastructural power. *Studies in Comparative International Development, 43*(3), 219–230. https://doi.org/10.1007/s12116-008-9030-z.

Subotić, J. (2016). Narrative, ontological security, and foreign policy change. *Foreign Policy Analysis, 12*(4), 610–627. https://doi.org/10.1111/fpa.12089.

ten Oever, N., Perarnaud, C., Kristoff, J., Müller, M., Resing, M., Filasto, A., & Kanich, C. (2024). Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine. *Policy & Internet, 16*, 692–710. https://doi.org/10.1002/poi3.422.

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian.* https://www.theguardian.com/world/2007/may/17/topstories3.russia

Tocci, N. (2021). Towards European cooperative autonomy. In R. N. Haar, T. Christiansen, S. Lange, & S. Vanhoonacker (Eds.), *The making of European security policy: Between institutional dynamics and global challenges* (1st ed., pp. 11–27). Routledge.

Vogel, T. (2011, March 23). Cyber attacks launched on EU computer systems. *Politico.* https://www.politico.eu/article/cyber-attacks-launched-on-eu-computer-systems/.

Von der Leyen, U. (2019). *A Union that strives for more: My agenda for Europe*. European Commission. https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en?filename=political-guidelines-next-commission_en.pdf.

Von der Leyen, U. (2023, September 13). *2023 State of the Union Address by President von der Leyen: Answering the call of history*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_23_4426.

Wagner, W. (2017). Liberal Power Europe. Journal of Common Market Studies, 55(6), 1398–1414. https://doi.org/10.1111/jcms.12572.

Weaver, D. (2020, June 30). Spatiality and World Politics. Oxford Research Encyclopedia of International Studies. https://doi.org/10.1093/acrefore/9780190846626.013.562.

Weber, V. (2020). *Making sense of technological spheres of influence*. London: LSE IDEAS. Retrieved from https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Technological-Spheres-of-Influence.pdf

Wendt, A. (1994). Collective identity formation and the international state. *American Political Science Review,* 88(2), 384–396. doi:10.2307/2944711.

Whyte, C. (2021). European Union policy, cohesion, and supranational experiences with cybersecurity. In S. N. Romaniuk & M. Manjikian (Eds.), *Routledge companion to global cyber-security strategy* (1st ed., pp. 123-138). Routledge. https://doi.org/10.4324/9780429399718

Wu, Z. (2017). Classical geopolitics, realism and the balance of power theory. *Journal of Strategic Studies, 41*(6), 786–823. https://doi.org/10.1080/01402390.2017.1379398

Zarakol, A. (2017). States and ontological security: A historical rethinking. *Cooperation and Conflict, 52(*1), 48–68. https://www.jstor.org/stable/48512930

Zhang, C., & Morris, C. (2023). Borders, bordering and sovereignty in digital space. *Territory, Politics, Governance, 11*(6), 1051-1058. https://doi.org/10.1080/21622671.2023.2216737.

Chapter 6 Appendix A – List of Interviewees

Formal interviews			
Interviewee code	**Date**	**Organization/Institution**	**Seniority**
A	05/03/21	EEAS, Lead cyber engagement and national representative	High
B	11/03/21	Permanent Representation of Estonia to the EU	Medium
C	12/03/21	European Council on Foreign Relations (Policy expert)	High
D	18/03/21	EEAS	High
E	25/03/21	European Commission – Executive cabinet	Medium
F	16/03/21	European Union Institute for Security Studies (Cyber Capacity Building Task Force)	Medium
G	9/09/22	(Former) Member State – United Kingdom, national government	High
H	15/09/22	European Union Institute for Security Studies, Cyber Policy	High
I	25/04/22	EEAS, Cyber Policy	High
J	30/05/22	European Commission, DG INTPA	Low
K	02/08/22	European College of Commissioners (Security Union)	High
L	10/05/22	EEAS, Secretariat General	High
M	06/05/22	European Commission, DG CNECT	High
N	06/05/22	European Commission, CC TT	High
O	31/05/22	Council of Europe (Cybercrime)	Medium
P	11/05/22	European Commission	High
Q	20/04/22	European Commission, DG NEAR	Low
R	17/05/22	European Commission, DG CNECT	Medium
S	16/05/22	EEAS, Eastern Partnership	Low
T	25/04/22	EEAS, Global Gateway	Senior
Q	15/04/22	(Former) Member State – United Kingdom, national government	Medium

Four Informal interviews: conducted over the 2022-2024 period, including a Lithuanian practitioner involved in the EU's PESCO cyber defence project, practitioners from the Global Cyber Security Capacity Centre (United Kingdom), and an interviewee formerly in the European Commission (DG Trade).

Chapter 7: Conclusion[69]

'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)

The dynamics of geostrategic behaviour in the digital age have not only emerged as a pressing subject in international relations scholarship, but they have increasingly pervaded our daily life. Yet, our prior grasp of geostrategic dynamics in and through cyberspace has been theoretically and empirically limited. This has led to significant gaps in our understanding about the emergence, drivers, and characteristics of geostrategic competition, especially in the case of the EU. This chapter foregrounds the key contributions of this dissertation to the field, beginning with its principal empirical findings and their wider significance to cyber-IR scholarship.

As I detail below, this thesis has examined the emergence and various manifestation(s) of the European Union's geostrategic behaviour in and through cyberspace, particularly the EU's evolving external action approach to digital sovereignty, capacity building, and spatial borders in and through cyberspace, and situates these developments within the global context of Sino-American competition. The dissertation's three articles developed novel analytical tools for approaching how and why core IR concepts (sovereignty, capacity, and geopolitics) have been represented and practiced by influential actors such as the EU, US, and China in differing ways, expanding and deepening our understanding of the nature of power and geopolitics in and through cyberspace. Based upon these findings, this conclusion chapter identifies further research directions which have emerged from this study, considers developments which have occurred after/outside the

[69] Parts of this chapter were adapted and pre-published as a short essay. See Julia Carver, '(Re)bordering Europe in the Digital Decade: Mapping the EU's development as a global cyber actor,' February 2024, *St. Antony's College.* Accessible here: https://www.sant.ox.ac.uk/wp-content/uploads/2025/03/Dahrendorf-Essay-Julia-Carver-latest-version.pdf.

scope of investigation of this thesis, and the wider implications of this project for our understanding of geostrategic behaviour in the digital age.

7.1. Key empirical findings

What explains and characterizes geostrategic behaviour in and through cyberspace? And what are the implications of these dynamics for the nature of sovereignty and geopolitics in the digital age? Collectively, this thesis demonstrates how contemporary geostrategic competition has been characterized by actors' efforts to build greater capacity in and through cyberspace by deploying a variety of hard (infrastructural) and soft (regulatory) tools. Counter to dominant accounts, I argue that this behaviour, particularly in the EU context, has been mediated by actors' ontological security drives and beliefs about the EU's role as a global cyber actor, not only material security concerns and cyber capabilities. Moreover, the EU's engagement with digital sovereignty discourse and practices towards cyberspace has been uneven and mediated by institutional and reputational variables, not only exogenous shocks.

Building upon critical and constructivist approaches to cyber-geopolitics, this thesis contributed empirical analysis and theoretical tools which have progressed the field beyond state-centric and 'power politics' studies of Sino-American competition premised upon technological superiority and cyber capabilities.

Chapter 2 elaborated the theoretical and empirical reasons for adopting this approach, emphasizing the limitations of IR literature that has positioned the EU as the 'geopolitical playground' rather than a 'geopolitical player' in its own right (Weber, 2020; Bradford, 2023). This approach has failed to anticipate and explain the EU's development as a geostrategic actor writ large, especially underexploring the global significance of the EU's development as a geostrategic global actor in and through cyberspace. Yet, growing

recognition about the EU's global importance in and through cyberspace is evidenced by its comparison to the United States and China as one of three competing 'digital empires' (Bradford, 2023) or 'digital hubs' (Drezner at al., 2021) in global affairs. Further, as Chapters 3 and 5 illustrated, cybersecurity issues have become increasingly prominent in the EU's external action approach, both in terms of legal acts, European Commission proposals, and joint publications with the EEAS. Thus, thesis has contributed to a greater understanding about the Union's strategic behaviour vis-à-vis the US and China in an increasingly digitalized global strategic environment.

In so doing, this thesis sought to denaturalize what it means to be a 'capable' (geostrategic) cyber actor by adopting a critical ontological approach to geostrategic competition and the concept of 'capacity' in the context of cyberspace. Here, I argued that we can further understand the geostrategic behaviour of global actors in and through cyberspace by returning to the foundations of 'capacity' as a foundation of power, and by drawing upon a critical, constructivist toolkit. This approach informed the three research articles comprising the thesis, which empirically examined and explained the EU's development as a global cyber actor through various angles of inquiry.

Emergence and drivers of geostrategic behaviour, especially in the EU context

By foregrounding the EU's emergence as a geopolitical actor, this thesis sought to advance mainstream debates about Sino-American geostrategic competition—which have tended to revolve around questions of territory and national determinants of power—towards including the EU's role and positioning as a geopolitical 'player' in and through cyberspace. To these studies, this dissertation advanced new empirical and theoretical claims regarding how state-based actors (viz. the EU, US, and China) engage cyber and digital instruments for broader geopolitical objectives.

Collectively, the articles demonstrated how ideational factors, including ontological security drives, competitive systemic pressures, and institutional variables have mediated the geostrategic behaviour of powerful global actors such as the EU, China, and the US. By comprehensively examining the drivers and consequences of mainstreaming cybersecurity into the domain of foreign policy, particularly in the context of EU external action, this dissertation advances efforts by cyber-IR scholars to 'integrate cyberspace with broader concepts and theories of IR' from the 'periphery into the core of the [IR] discipline' (Foulon & Meibauer, 2024, p. 426).

Specifically, Chapter 4 of my dissertation is the first (to my knowledge) to identify an influential convergence between geostrategic thinking and *external capacity building assistance* in cyberspace provided by powerful donors (viz. the United States, China, and the EU). This paper developed a theoretical framework of networked competition to explore how the EU, US, and Chinese foreign policy discourses have constructed capacity building assistance for digital development as geostrategically important. In accordance with my theoretical argument, my empirical analyses of US, Chinese, and EU provisions of capacity building assistance for African states' digital development have appeared to conform to a strategic, competitive logic. To conceptualize and explain variation in the type of capacity building instruments provided by Washington, Brussels, and Beijing to recipients, my analysis highlighted three significant factors: the donor's normative approach to development, their relative access and control over the intermediary, and the presence of geopolitical competitors. Accordingly, Chapter 4 demonstrated that existing explanations about the strategic logic(s) of digital and capacity building are insufficient, as evidenced by the growing convergence between capacity building and geostrategic competition in the digital age. Rather, contemporary international development cooperation has been characterized by the integration of cybersecurity instruments with digital development

policies in multiple foreign policy contexts, including the EU, US, and China, as well as non-state actors, and with the growing 'infrastructural' dimension to cyber capacity building provisions in Western contexts.

In turn, Chapters 5 and 6 delved further into the drivers and characteristics of the EU's specific geostrategic turn in and through cyberspace. Chapter 5 explored the extent to which European digital sovereignty discourse drove the development of cyber instruments which have operationalized Brussels' control over the digital domain. Specifically, it focused upon three significant policy developments: the EU's Cyber Diplomacy Toolbox, EU external cyber capacity building programmes, and the 5G Toolbox, all of which have overlapped with the emergence of European digital sovereignty discourse in EU external action policy. Rather than this discourse driving all three policy changes, my findings revealed that European digital sovereignty discourse comprehensively shaped changes to the 5G Toolbox, yet it had an inconspicuous relationship to the other two cases of significant policy change. Drawing upon my discursive-institutionalist framework, I argued that the varying influence of European digital sovereignty discourse was conditioned by the EU's existing external action competences, reputational concerns, and (perceived) legitimacy issues.

Next, drawing upon ontological security and critical geopolitics scholarship, Chapter 6 demonstrated that the EU's ontological security drives have conditioned the EU's engagement with spatial (b)ordering practices—and thereby the parameters of the Union's role as a global cyber actor—over time. Particularly, the EU has consistently deployed spatial (b)ordering moves to demarcate, practices, and routinize its role in cyberspace vis-à-vis others. At the same time, such spatial (b)ordering moves have sought to manage the EU's efforts to adapt to an evolving strategic context and the challenges these crises have posed to the Union's ontological security. By foregrounding the overlooked dimension of

ontological security drives, this account challenges the assumptions of mainstream scholarship about geopolitical competition, which have privileged systemic level shifts, material security concerns, and realist conceptions of 'geopolitical power' to assess changes to the EU's role as a global actor above ideational and endogenous variables. Rather, I show how the EU's global role in and through cyberspace has evolved *dialectically* with structural changes to the global cyber and wider strategic environment(s), an ongoing process underpinned by the EU's quest for ontological security.

The chapters also highlighted dynamics of cybersecurity policy integration in practice. For example, Chapter 5 traced the dual mainstreaming of 'European sovereignty' discourse with 'cyber policy' in EU external action and the close intertextuality between cyber and digital policy issues across multiple areas of EU external action. Meanwhile, Chapter 6 explored dynamics of cybersecurity integration from a different angle by analysing key policy developments in the EU's evolution as a global (geo)strategic cyber actor over the 2009-2024 period. Therefore, the articles also offer substantive contributions to EU studies, as they reveal how a key characteristic of European integration appears to be reproduced in the context of the EU's cyber-external action approach: the significance of spatial (b)ordering for mediating adaptations to the EU's role construction as a global cyber actor over time. For instance, my analysis in Chapter 6 demonstrated how the EU's self-representation of its 'sovereigntist' and 'geopolitical' role in and through cyberspace reproduces its longstanding 'supranational temptation' (Neumann, 1998, p. 413) to stabilize the Union's collective sense of self by 'borrowing from traditional nationalist forms of othering' (Klose, 2023, p. 581). Accordingly, this thesis suggests that the integration of cyber instruments into wider foreign policy objectives, including geostrategic competition, may be conditioned by an actor's ontological security drives.

More importantly, as I discuss below, the empirical claims of this dissertation have wider relevance for cyber-IR scholarship in several ways.

7.2. Sovereignty, geopolitics, and territoriality in cyberspace revisited

This thesis has empirically identified several contemporary dynamics of geostrategic competition, including the integration of cyber and digital instruments into wider geostrategic objectives (such as cyber and digital capacity building), the operationalization of cybersecurity instruments for digital sovereignty objectives, and the EU's changing strategic approach to cyberspace. What, then, are the implications of this study for our thinking about geopolitics and sovereignty in theory and practice, including in and through cyberspace? I discuss several broader implications below.

The EU as a geostrategic actor in cyber-IR

Foremost, my thesis challenges the state-centric and materialist bases of mainstream IR theory by developing alternative theoretical and empirical approaches to conceptualizing the EU as a geostrategic cyber actor. Realist, state-centric, and capabilities-based accounts fail to explain the ambitious geostrategic behaviour of non-traditional actors, such as the European Union, which lacks the coercive trappings of a 'capable' actor and currently suffers from a 'technological deficit' (Borrell, 2024). Thus, by examining the supranational level of EU external action policies in and through cyberspace, this dissertation has unveiled a largely overlooked level of analysis to geopolitical competition in and through cyberspace. As noted in Chapter 2, mainstream accounts have positioned Europe (especially the EU) as ancillary to the competing US-China power struggle for geopolitical and technological superiority in cyberspace (see also Bradford, 2023; Weber, 2020). In this vein, scholars have chiefly drawn upon *intergovernmentalist* theory, which may be situated within the realist paradigm, to theorize about the scope of EU cyber strategy development (Hix, 1994). 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 (Hoffmann, 1996).

The significance of the EU as a relevant cyber-geostrategic actor in its own right is evinced by the prevalence of cyber and digital capacity-oriented discourses within and across EU institutions, as explored in Chapters 4, 5, and 6. Chapters 4 and 6 highlighted the growing 'infrastructural turn' in the EU's external cyber capacity building policies and its rising strategic importance within the EU's wider approach to digital development. Further, Chapter 5 explored three policy changes which sought to operationalize greater EU control and authority over space through cybersecurity instruments. Chapter 6 further identified the EU's longstanding discursive association of cyber insecurities with the EU's *capacity* to fulfil its Internal Market functions and 'responsibilities' as a global actor. Altogether, the research articles have foregrounded the significance of external capacity building (in Chapters 4,5,6) *and* internal capacity building (as the capacity to act, in Chapter 6) for constituting actors' geostrategic behaviour.

By clarifying the institutional and ideational foundations to the EU's geostrategic turn, including through the perspective of EU actorness (as in Chapter 6), the findings of this thesis challenge the treatment of the EU as a 'geopolitical playground' rather than a geopolitical player, and by extension, pure intergovernmentalism. 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 2014, p. 470), Chapter 5 revealed how, despite competing Member State conceptions of the term, national sovereignties have *not* precluded the development of the 'European sovereignty' concept. Rather, as Chapter 6 argued, 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.

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, this thesis revealed how attributing this move on the basis of pure intergovernmentalism is unconvincing. This account is challenged by the reality that the Union lacks hard power resources, including the EU's cyber-force capabilities, and the significant involvement of supranational actors, including the European Commission, in shaping the collective (re)imagination of the EU's global role in and through cyberspace since 2009. Indeed, Chapters 5 and 6 have laid bare the significant extent to which influential discussions about cybersecurity in Europe have been held above the national level, demonstrating that Member States' motives are not the only drivers of this European sovereignty narrative. That is, 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.

Accordingly, this research builds upon work in EU studies which has elaborated the significance of a 'EUropean geopolitical imaginary' for EU policymaking (e.g. Csernatoni, 2022; Monsees & Lambach, 2022). This imaginary is constructed through spatial (b)ordering moves by multiple supranational institutions (viz. EEAS, the Council of the EU, and the Commission), using various discursive and policy instruments which establish an internal EUropean (cyber)space and external outside. European digital sovereignty discourse has been instrumental for constructing this imaginary: Chapters 5 and 6 demonstrated how this discourse has sought to both differentiate the Union from Others and to encourage EU actors' cohesion around a '*EUropean'* internal (cyber)space.

While modernist conceptions of geopolitics in IR are premised upon territorial (national) sovereignty as a precondition for issuing geopolitical claims, the EU's emergence

as a geostrategic actor complicates these accounts. I have argued that the EU's expression of digital sovereignty conveys both an assertion of authority over European cyberspace and an external claim to legitimate the EU's role as a *geopolitical a*ctor in its own right. While this vision is *territorializing*, in that it entails the demarcation of (cyber)space, it does not unfold neatly in line with nation state boundaries—rather, it also incorporates aspects of internal *debordering* (e.g. between Member States) and elements of networked competition, such as through capacity building assistance. Furthermore, the EU's geopolitical imaginary is self-consciously *Europeanizing,* revolving around the assertion of the Union's values vis-à-vis significant others. Former European Council President Charles Michel positioned the EU's approach to digital sovereignty as somewhere '*between* an unregulated model and a state-controlled model [that] promote[s] a human-centric, ethics-based approach, that serves our citizens,' (emphasis added, European Council, 2021). This reflects the EU's efforts to advance a distinctly 'European approach' to digital sovereignty and strategic autonomy, walking the tightrope between the US and Chinese approaches towards the internet (Falkner et al., 2024).

Critical geopolitics scholars have likened the use of geographic frames to the concept of 'geopolitical' or 'spatial' imaginaries (see for example Branch, 2024). Particularly, geopolitical imaginaries, scholars have demonstrated elsewhere, are linked to states' construction as 'imagined' communities (Agnew, 2004). Accordingly, creating an 'imagined' (bounded) cyberspace can be understood as another form of state or capacity building process in and through cyberspace (see also Bridges, 2024). By examining the context of cyberspace, this thesis contributes novel empirical evidence to critical geopolitics scholarship on the ontological security foundations to geopolitical behaviour (see for example Agnew, 2004; Eberle & Daniel, 2022). As I demonstrated in the case of the EU,

expressing geostrategic claims, including digital sovereignty discourse, is mediated by ideational factors, including an actor's (past) self-construction in this context.

More broadly, the findings of this thesis suggest that further research should be devoted to exploring various instantiations of geostrategic behaviour beyond the nation state context, including the expression of sovereigntist frames by Big Tech actors. Recently, powerful companies such as Microsoft, Amazon, and Oracle have advanced several products which claim to provide sovereignty services, such as 'Microsoft Cloud for Sovereignty' (Microsoft, 2025) and Oracle's 'Sovereign Cloud Services'. As governments continue to invest in building their 'digital' and 'cyber capacity', including by investing in such services, there is a wider imperative in IR to scrutinize geostrategic behaviour within and beyond the state. This thesis has developed several theoretical tools to investigate geostrategic competition beyond mainstream approaches which could be potentially be applied to these cases, including a spatial (b)ordering framework, a critical ontological approach to concept analysis, and a framework for networked competition.

Capacity as a theoretical and practical dimension to geostrategic competition

Second, this thesis foregrounded the 'double nature' of capacity as a strategic concept in cyber-IR. In Chapter 2, I argued that, despite the foundational role of state capacity for developing, integrating, and using cyber capabilities for strategic purposes (Slayton, 2016), as well as the foundational role of capacity for an actor's sense of self and agency (Krickel-Choi, 2022; Klose, 2018), there has been little academic scrutiny directed towards 'capacity' in cyberspace as a theoretical and practical concept. Rather, to anticipate and explain strategic competition in the digital age, mainstream international relations ('cyber-IR') approaches have centered around an actor's possession of cyber capabilities (McCarthy, 2015), and/or an actor's leading technological position in 'high technologies',

such as artificial intelligence and computing (Ding, 2024), which have led to a limited understanding about geostrategic behaviour in the context of cyberspace. Meanwhile, critical and constructivist scholarship has highlighted the co-constitutive, sociotechnical character of 'cyberspace' (and thus the nexus between politics, humans, and technological change). Yet, this literature has failed to unpack the destabilizing influence of digitalization and cybersecurity threats to the state's sense of Self and its capacity to provide public goods for its citizens, thus triggering ontological security management behaviour. In brief, we lack an adequate understanding about the material and existential foundations of (state) capacity and its evolving relationship to strategic competition in the contemporary digital age.

As a first step to resolving these empirical and theoretical gaps, in Chapter 2 I argued that we should examine 'capacity' as a theoretical and practical concept vis-à-vis cyber geopolitics more closely. Through a critical ontological lens, I theorized that an actor's capacity to act in and through cyberspace can be approached as a 'basic' concept in international relations and differentiated at two levels: 1) the level of academic research and abstract reasoning; and 2) the level of practice and/or everyday life (Berenskoetter, 2017, p. 155). In other words, I argued that 'capacity' is a significant concept at the level of academic research on cyber-geopolitics (e.g. as an analytical category, or as a tool for abstract reasoning) *and* in the context of everyday life, as a 'category of practice' for policymakers (Berenskoetter, 2017, p. 155).

Indeed, the findings from my research articles suggest that capacity functions both as a *rationale* for strategic decision making in practice *and* as a significant analytical category. On the one hand, my findings demonstrated how an actor's 'capacity', as an academic concept, can serve as a meaningful precursor for projecting power in cyberspace in the form of control and boundary (re)definition in and through cyberspace. In Chapter 4, I theorized that the EU, US, and China have perceived their relative positionality within and

across digital networks as strategically important, wherein digital and cyber capacity building assistance initiatives were perceived by powerful donors as forms of strategic alignment, which could be calibrated between the donor and recipient through a variety of capacity building instruments. While there was a clear structural dimension to this positioning, the paper also emphasized the significance of donor perceptions and demonstrated that cultural and ideational variables played a role in shaping donors' varied use of particular capacity building instruments in their assistance programmes. Next, Chapter 5 examined the relationship between the EU's enhanced capacity to achieve control and authority over the global digital domain through cyber instruments (exemplifying 'European digital sovereignty' in practice) and high-level expressions of European digital sovereignty discourse. Finally, Chapter 6 explored how the 'capacity to act' in and through cyberspace has become closely associated to the Union's sense of agency as a global actor, conditioning EU actors' engagement with sovereigntist logics and bordering practices in and through cyberspace. This chapter underscored the agentic dimensions and ontological security drivers of geostrategic behaviour in cyberspace—that is, how actors (re)imagine their roles and position(s) in cyberspace vis-à-vis others.

Collectively, these chapters revealed a *capacity building* trend in EU cyber policymaking, thereby contributing to recent EU Studies debates about the 'state-building' turn in EU cybersecurity policy (Farrand et al., 2024). This builds upon a small, nascent body of scholarship which has illustrated the influence of EU's geostrategic approach on the evolution of several cyber-relevant policy areas, including artificial intelligence (Mügge, 2024), cyber defence (Backman, 2023), online content control (Flonk et al., 2024), Domain Name System governance (Radu, 2023); global internet governance and sanctions (ten Oever et al., 2024), among others. In so doing, this dissertation redressed several remaining empirical and theoretical gaps in this sub-field, including the territorial, ontological, and

(geo)spatial underpinnings of the Union's development as a global cyber actor and the importance of capacity building as a relevant analytical concept for EU policymaking.

Ultimately, this thesis revealed how the concept of capacity serves multiple purposes in the practice of cyber-IR. On the one hand, as an actor can *intentionally* take steps to prioritize aspects of building their capacity, capacity constitutes the material and socio-political conditions (e.g. competences) which can enable or constrain action. At the same time, an actor's real-life assumptions about capacity inform particular rationales about what it means to be a 'capable' actor in a given context, and it can serve as a strategic frame to promote particular policy tools. Therefore, capacity building projects can serve as indicators for how actors perceive the prioritization of particular resources and competences to fulfil their strategic objectives. Accordingly, these findings contribute to critical/constructivist approaches to ontological theorizing in IR, also known as the 'linguistic turn'. As Berenskoetter maintains, there is a considerable overlap between academic and socio-political conceptual language, particularly 'basic' concepts such as the 'state' and strategic concepts such as the 'balance of power' (2017, pp. 156). Indeed, much like the 'knowledge producing' nature of geopolitical thinking (Agnew & Corbridge, 1995), notions of 'cyber-' and/or 'digital capacity' bleed from practice to academic research, and vice versa. Overall, leveraging capacity as an analytical concept serves as a valuable alternative point of departure for future research concerned with how actors compete for influence in the current digital age, including how actors perceive their own relative power (and weaknesses)—which could complement existing work on cyber capabilities.

Liminality as a characteristic of geostrategic competition

By exploring the above dynamics, this thesis has exposed the *liminal* nature of geostrategic competition in and through cyberspace; a dynamic broadly characterized by 'in

betweenness' and adaptation (Adams & Warf & Wharf, 1997, p. 161). At a structural level, the sociotechnical features of cyberspace and their potential for (re)construction through structural developments, including the construction of digital infrastructure (as in capacity building programmes), facilitates the fluidity and liminality of space and place. These liminal features have been widely recognized as contributing to the domain's strategic uncertainty (Dunn Cavelty & Wenger, 2022), exacerbating ontological challenges about the domain's basic features and risks (Lupovici, 2023), and as evoking emotional and/or biased responses to cyber events (Gomez, 2019; McDermott, 2019). As I demonstrate in this study, the liminal, 'borderless', yet interconnected characteristics of cyberspace have exacerbated actors' fears of digital dependence and encouraged both states and supranational actors to engage in spatial (b)ordering efforts to manage insecurities about the basic features of the cyber environment. Efforts to 'journey from space to place' (Adams & Warf, 1997, p. 161)—and therefore exercise sovereignty claims over a specific, bounded area—are complicated by the rapidly evolving environment and complex territoriality of cyberspace. Yet, as Chapters 4 and 6 revealed, these same features can generate opportunities for actors to engage in creative action through spatial (b)ordering moves—possibilities which have been integrated into actors' wider geostrategic agendas.

Alongside spatial liminality, Chapters 5 and 6 demonstrated that the EU's geostrategic behaviour in and through cyberspace–as a process of role (re)construction–has been characterized by dynamics of *temporal* liminality, between the EU's past and present 'selves' as a global actor. For example, as I argued in Chapter, 6, the EU's self-narrative as a global cyber actor has sought to both reproduce and transcend its past self-image: reinforcing its past role as a global technological leader by adopting new forms of spatial ordering and control and a new 'mindset' to global interdependence. In this way, it can be understood that the EU has currently positioned itself in a state of 'betweenness': between

embracing an orthodox geopolitical approach and its historical commitment as a liberal global actor. As Merje Kuus avers, 'even claims about "escaping" geography and geopolitics are geopolitical insofar as they assume a particular geographical configuration of power that is to be eluded,' (2007, p. 7).

Accordingly, my empirical analysis indicates that these two dimensions of liminality in the argument are related. If cyberspace is constantly characterized by technological changes, structural adaptations, and strategic uncertainty, its spatial liminality may be inherently unsettling for traditional state-based actors, and encourage actors to refer to past practices and roles whilst seeking to overcome them at the same time. As Chapters 4 and 6 have explored, various global actors, including the EU, have sought to exert functional and territorial control over cyberspace through various attempts to 'settle it', by exporting their own models of governance, ideals/norms, and technologies. Chapter 6 suggested that the Union's spatial (b)ordering moves in and through of cyberspace may constitute efforts to manage the EU's sense of dislocation between 'envisioned' (physical space) and 'experienced' space (see also Lupovici, 2023). Elsewhere, Branch has demonstrated that the United States' association of 'cyberspace' with the military 'domain' concept, 'allowed convincing parallels to be drawn to physical spaces' and to military and operational rationales (2021, p. 48). Similarly, my study demonstrated how key EU actors have mobilized arguments about 'cross-border' risks and insecurities to link cyberspace with familiar arguments for further European integration, particularly in the context of economic security policy and international cooperation. These cases evidence how institutional actors have engaged routinized spatial (b)ordering moves to manage the unsettling nature of cyberspace by framing it in terms of familiar past routines, rationales, and imaginaries.

Digital dependence and ontological security drives

Finally, this thesis has theorized a significant relationship between anxieties about digital dependence and ontological security management behaviour. Chapter 6 explored how the EU's fears about weaponized interdependence, including in and through cyberspace, evinced a fundamental 'shift in mindset' (Borrell, 2023) in the EU's conception of the future global environment—and thereby in the EU's imagined role as a global actor vis-à-vis others, including the United States. The chapter traced how anxieties about the evolving global environment, including the Union's digital dependence vulnerabilities, rising cyber insecurities and adversarial subthreshold activities, have disrupted the EU's capacity to maintain a sense of 'self' through 'being' and 'doing' in a constantly changing environment,' (Flockhart, 2016, p. 805). These instabilities, I argued, have triggered EU spatial (b)ordering moves, which seek to stabilize the Union's environment in line with a comforting image.

Existential anxiety is, after all, the 'sense that the future will be unlike the past in ways we can hardly conceive of, much less control,' (Kinvall & Mitzen, 2020, p. 245). Indeed, Chapter 6 demonstrated how weaponized interdependence discourse has aggravated the EU's deep-seated fear of 'falling behind' as a 'high tech' leader, which would depress the EU's capacity to shape the future and undermine its self-representation as a cultural and technological leader.

Exploring the relationship between weaponized interdependence discourse and anxieties about the future complements existing international political economy scholarship, which has interrogated the material basis (and credibility) of weaponized interdependence as a strategic concept. This literature has emphasized vulnerabilities to coercion and sabotage determined by the actor's strategic position in asymmetric networks (Farrell & Newman, 2019; Drezner et al., 2021). Yet, by mobilizing an ontological security-informed framework, as developed by Chapter 6, it can be understood that invoking the concept of weaponized

interdependence expresses not only structural risks and material realities, but an actor's inherent beliefs about the future and their place within it.

Under these conditions, my dissertation unveiled how European digital sovereignty discourse appeared to respond to digital dependence anxieties and ontological insecurity drives. This suggests that, so long as weaponized interdependence concerns remain an in-vogue policy concept, the EU may continue to adopt sovereigntist and other geostrategic posturing, including mercantilist economic policies, which aim to redress the Union's perceived vulnerabilities arising from global interdependence. However, this trend is more widely observable across different geographic contexts – as noted in Chapter 4, concerns about 'digital dependence' have driven calls to protecting African states' sovereignty (African Union, 2020). Further research could apply an ontological security lens to digital dependence discourses in contexts beyond the EU, as a dimension of contemporary geostrategic competition. Consequently, this thesis sheds light on all three 'qualities' of geopolitics, as laid out by Klaus Dodds: 1) traditional questions about the 'territorial interests and power of the state'; 2) interpreting/understanding global affairs through 'geographical frames'; and 3) future-oriented concerns related to geographic control and the question of borderlands (Dodds, 2019, p. 6).

7.3. Study limitations

As detailed in Chapter 3, all three articles in my integrated thesis adopted distinct qualitative research designs and leveraged primary source documents and elite interviews. My analysis was careful to identify how different document types—from internal memos, staff guidance, to official speeches, doctrines, and legal acts—are produced with different internal/external audiences in mind, which could shape the vocabulary used. For example, to examine and identify Chinese sources for Chapter 4, I was reliant upon Chinese primary

sources published in English, or on translations of Chinese strategic concepts and internal debates published by secondary literature, which provided a more limited view of how the PRC rationalizes capacity building assistance to its domestic audiences and in internal policy debates. However, even internal public documents could mask invisible areas of contestation or internal incoherence in various policy contexts. This limits the inferential leverage of the study; a point which will be further elaborated in this section.

As I discussed in Chapter 3, the relationship between 'thinking, saying and doing' is often challenging to gauge, as agents may not say or do what they're thinking, and vice versa (Schmidt, 2011, p.115). Accordingly, the thesis sought to situate the interviewees (and their responses) in context and it undertook various methods to assess the trustworthiness of the data (such as intertextuality, exposure, transparency, and reflexivity). For example, to corroborate my discourse analysis and identify any gaps or tensions between official documents and internal debates, I also conducted elite interviews with key policymakers and policy experts. These interviews were beneficial for exploring, albeit in a limited way, ideas or issues that are 'invisible' official/public documents. At the same time, elite interviews may introduce potential risks of response bias and are subject to my interpretation and positionality as a researcher/interviewer. Particularly, interviewees' positionalities shape their perspectives, experiences, and understandings of particular issues / question prompts, such as the meaning of concepts as 'European digital sovereignty'. Since the majority of my interviewees comprised current or past employees of EU institutions (e.g. the European Commission, the Council of the EU, and the EEAS) at varying levels of seniority, and some EU Member States, the inferential leverage of the interview data is limited to these contexts.

Nonetheless, interviews and primary course documents were important to exploring a key empirical thread of this thesis, which has focused upon how various institutional actors and/or governments represented cyber issues as *particular* types of problems (Bacchi &

Goodwin, 2016). Based upon its three research articles, this chapter argued that cyber-geopolitics has been characterized by 'liminality', or a conceptual environment of 'in betweenness'—both recasting and reclaiming the logics, means, and methods used by its earlier predecessors.

One might further object that examining the varied meaning(s) of 'cyber' and 'digital' issues over time and across institutional contexts could run the risk of conceptual stretching and/or confusion between the conceptual developments in the field of cyber studies and the actual verbiage of cyber and digital issues in certain policy contexts.[70] As discussed earlier in this chapter, the ontological approach of this thesis was to expose, not subsume, these conceptual and theoretical issues. Embracing this conceptual fluidity and fuzziness reflected a key objective of this thesis, which was to identify and problematize the convergence between cyber strategies and geostrategic behaviour from the perspectives of various policy actors. Moreover, this contestation is one consequence of the transversal, complex 'politics of cybersecurity' (Dunn Cavelty & Wenger, 2022) and its practical integration with classical IR concepts. Exploring these conceptual debates, including the 'repackaging' of cyber policies under new strategic objectives (as identified in Chapter 5, for example), has produced novel insights about the areas of discursive contestation and debates over the meaning of key cyber issues, which in turn reveals the evolution of cyber strategy vis-à-vis geopolitical and sovereigntist goals. However, it also implies that the generalizability of this research is necessarily limited.

A corollary of this approach, as discussed in Chapter 3, is that it does not offer a universal or exhaustive overview of all policy cases or instruments inherent to cyber-

[70] Here, one could ask: are cyberspace and the digital domain one and the same? Throughout this thesis, I have approached this question by examining how the EU and other actors define these two concepts in various policy contexts. Chapter 4 notes the siloed approach to cyber versus digital capacity building by the cybersecurity and global development communities, while, as I note in Chapter 5, the EU's external action approach conceives of the digital domain as *including* cyberspace and cybersecurity instruments, although this conceptualization could change over time.

geopolitics and/or sovereignty in and through cyberspace. This thesis examined the convergence of cybersecurity instruments with the EU's (geo)strategic objectives in four of six areas of EU external action,[71] namely commercial (trade) policy; development cooperation; economic, financial and technical cooperation with non-EU countries; and the common foreign, security and defence policies (CFSP and CSDP). Regarding the two sub-areas of external action not covered by the thesis, there is little research on how the EU's geostrategic ambitions in and through cyberspace bear upon humanitarian aid, which could point to an important research gap not covered by this thesis. Elsewhere, scholars have explored the EU's (geo)strategic approach to borders using digital and cybersecurity instruments in the sub-area of migration policy (see for example Broeders, 2007).

Furthermore, since the scope of the analysis focused upon the EU level, rather than the Member State level, it did not capture national-level debates about digital sovereignty and/or geopolitics in depth. While Chapters 5 and 6 explored horizontal and vertical contestation in various EU cyber policymaking contexts, as well as the strategic (national) discourses of more capable EU member states (e.g. the UK during its membership, France, and Germany), they focused upon specific policy areas, not on the wider national contexts per se. These articles have also recognized the potential significance of Member State 'uploading' to the EU policy level, while maintaining the rationale for approaching their research questions from the perspective of an EU-level external action context (for further discussion, see Chapter 3).

A Member State-forward approach, in turn, would have likely captured more intergovernmental bargaining dynamics relevant to evolving relationship between geostrategic tools in and through cyberspace, as well as their varied application. For

[71] As noted in Chapter 3, EU external action entails six policy dimensions: commercial (trade) policy; development cooperation; economic, financial and technical cooperation with non-EU countries; humanitarian aid, the common foreign, security and defence policies (CFSP and CSDP); and the external dimension of other EU internal policies (e.g; migration).

example, examining the extent to which certain cyber policy ideas have been 'uploaded' to the EU supranational context, and their relationship to the EU's evolving engagement with geostrategic concepts in and through cyberspace, would be a valuable complement to this research, and could contribute to developing and testing out several EU-level institutional and ideational dynamics identified by Chapters 5 and 6. Potentially, such an approach could reveal more insights about the relationship between member state and European sovereignty(ies), as opposed to the EU's role as a *sui generis* global cyber actor, which is an adjacent question and phenomenon explored by this study. Therefore, focusing upon Member State perspectives and spotlighting the vertical dimensions of EU cyber governance, for example, would also be complementary to this study and it represents a promising area for future research.

On a similar note, the dissertation's empirical coverage largely omitted the practical transposition or implementation of EU policies into national contexts, which could serve as an alternative measure of examining EU digital sovereignty measures in practice and at the Member State level. Rather, the dissertation was primarily concerned with the meaning and evolution of (geo)strategic concepts, such as digital sovereignty, weaponized digital interdependence, and networked competition, and their association with/to cyberspace and cyber issues in different policy areas.

Given the dissertation's primary research objectives, the transposition and effectiveness of EU cyber policies were often (but not completely) outside of the primary scope of the dissertation's research aims for several reasons. First, the thesis focused heavily upon the EU's external action policy domain (or indeed US and Chinese foreign policy developments), including digital development, which often transcended the scope of EU domestic implementation (as in Chapter 4). Second, some of the developments examined by the chapters are too recent (e.g. in Chapters 4 and 5) to draw credible conclusions about the

effectiveness or implementation of these policy instruments. Third, evaluating the effectiveness of EU policy changes at the Member State level is further hindered by the reality that the strategic concepts goals (sometimes) associated with EU cybersecurity policies, such as digital sovereignty discourse, and/or distinctions between 'cyber' versus 'digital' development issues, vary in meaning across trans/national contexts (see Chapters 4 and 5; see also Rone, 2024). Both of these factors makes it difficult to predict how such policies may be implemented or conceptualized across different policy contexts and over time. Nonetheless, the thesis did explore these issues with respect to earlier/past EU cyber policies, where relevant.[72]

Furthermore, the thesis did not explore EU-NATO relations in depth, which could serve as both a research limitation and a future opportunity for further study. The thesis did not squarely focus upon cyber defence issues, but rather several other areas of EU external action (including CFSP), there is a high degree of overlap in European states' membership in NATO and the EU, respectively. Additionally, there is considerable diplomatic overlap between EU-US transatlantic relations on tech-related issues and EU-US cooperation in NATO. As noted in Chapters 5 and 6, the EU and the US have longstanding relationships in the areas of cybersecurity and technology, whereby the US has been considered for a long time the EU's closest partner on cyber issues. Further research could be placed upon EU-NATO relations, particularly in the context of cyber defence—an area of EU external action that was not examined in depth by this thesis.

[72] Leveraging primary source documents and elite interviews, Chapter 6 explored the vertical and horizontal contestation over the development of the EU's strategic approach to cyberspace over time (beginning in the 2010s). These issues were approached from the perspective of competing discourses and perspectives of the EU's role and capacity to act in and through cyberspace, in line with the paper's exploration of the relationship between the EU's sense of self and its changing engagement with spatial (b)ordering moves in and through cyberspace over time.

Here, it is further worth noting that, while NATO is a transatlantic security alliance, the EU's external action approach to global cyberspace transcends the 'hard' security context and intergovernmental decision-making within the NATO framework. Nevertheless, it is possible that socialization between non-EU states in NATO and EU Member States may affect the development of EU cybersecurity policy. Given the relevance of institutional context identified by Chapter 5 in the formation of the EU's geostrategic approach to cyberspace, I would expect that the influence of NATO-based socialization on the EU's approach to cyberspace is likely to be stronger in the area of cyber defence than other areas of cyber-relevant foreign policy, although this requires further research. Alternatively, EU-NATO relations could also serve as an external shock or relational influence upon the EU's geostrategic self-positioning in and through cyberspace. In this regard, EU-NATO cooperation should not be dismissed an influence on the EU's global approach to cyberspace, and it represents an important area for future analysis.

Consequently, the findings of the thesis should not be decontextualized for the purposes of drawing wider conclusions about the future of EU-NATO relations in and through cyberspace. After all, the findings of this thesis have demonstrated the complexity of EU-US transatlantic relations across different cyber-relevant foreign policy areas. As Chapter 4 demonstrated, the EU and the US have competed in the context of digital development, advancing competing capacity building assistance frameworks, including at the governance and sectoral/skills building levels geared towards promoting 'European' *or* 'American' approaches. At the same time, Chapters 5 and 6 evidenced how EU-US diplomatic relations, including partnerships in cyber relevant issue areas, have long been integral to the EU's positioning as a global (cyber) actor. These dynamics overlap with the wider strategic context, including relations within NATO. However, the distinctive effect of EU-NATO relations on the EU's geostrategic approach remains difficult to disentangle.

In sum, by shedding further light on several under-researched policy areas, including capacity building assistance and the development of the EU's cyber strategies over time, the preceding chapters sought to challenge existing accounts and draw out wider insights about the drivers and key discourses, practices, and instruments underlying geostrategic behaviour in and through cyberspace. However, they do not provide an all-encompassing view of all possible variants of geostrategic behaviour in and through cyberspace. Overall, the articles privileged greater depth of focus and empirical richness over breadth (oriented around better understanding the nature of geostrategic behaviour in overlooked foreign policy contexts), which led to some compromises on generalizability, as discussed more specifically in the articles.[73] By the same token, this thesis introduces multiple fruitful pathways for future research, and its insights may help us to approach and understand future global trends. Below, I further highlight five promising research avenues.

7.4. Avenues for future research and recent global trends

The findings of this thesis reveal five fruitful avenues for future research in IR regarding the nature of geopolitical competition in the digital age, and the EU's role as a global actor. Foremost, Chapter 4's research on the African digital development context demonstrated how so-called "peripheral" areas of the network have played a significant role in the dynamics of great power competition in the digital domain. This study provides a clear

[73] As discussed in the articles in more detail. For example, Chapter 4's theoretical framework is premised strongly upon the supply-side dynamics of digital development. On the one hand, it revealed greater insights about the convergence of cybersecurity issues, digital development policy, and strategic competition in the context of EU, US, and Chinese assistance provisions towards African states. Due to scope and length constraints, the article therefore offered a limited view of demand-side or beneficiary perspectives towards such assistance. Accordingly, further research could apply and adapt the article's theoretical framework to other country contexts, especially in terms of the recipient side to digital development. Separately, Chapter 5 engaged 'explaining-outcome process tracing', or an abductive, eclectic, and bottom-up method, in which the researcher begins with an outcome and recursively examines the evidence to explore which factors appear to have driven the phenomenon of interest in each case (Beach & Pedersen, 2019; Haroche, 2022). While this approach provides fruitful opportunities to mobilize new theoretical tools to explain complex problems, including discourse analysis (Beach and Pedersen, 2019, p. 282, in Haroche, 2022), the generalisability of such an approach is limited. Similarly, the empirical focus of Chapter 6's qualitative-interpretive approach is limited to the EU context, as discussed earlier.

pathway for future research on geopolitical competition, which has largely privileged ‘great power’ contexts, such as ‘decoupling’ the American market from Chinese technologies (e.g. Kokas, 2022), over developing parts of global cyberspace. The nexus between geopolitical competition, structural and ideational changes to cyberspace, and capacity building assistance remains an underexplored area of research, despite its rising global importance as a foreign policy tool (see also Collett & Barmpaliou, 2021). Accordingly, further research can explore the positioning of developing states and ‘middle powers’ in this context, and their perceptions about the strategic import of partnerships in and through cyberspace.

Considering these developments, another ripe area for further research concerns the relationship between capacity building, strategic partnerships, and international security governance. Sukumar, Broeders and Kello (2024) have observed elsewhere the rising proliferation of ‘informal governance in international cybersecurity’, whereby global actors, including states and non-state actors, have preferred informal settings to discuss cyber governance issues to formal multilateral cooperation. Notably, Sukumar et al. argued that the rise of ‘multipolar geopolitics coinciding with a general decline of formal multilateral cooperation’ has served as a major driver of the ‘stickiness’ of informal international cybersecurity governance regime (2024, p. 11). They argued that geopolitical tensions, including concerns about digital vulnerabilities (as evidenced by the 5G debate) have constrained and mediated debates in the UN. How could the increasing strategic salience of external capacity building assistance tools—including for geostrategic competition—relate to this ‘pervasive informality’ in cyber-IR? As explored in Chapter 4, the Biden Administration’s strategy of building ‘digital solidarity’ with other actors—an objective primarily pursued through infrastructural and human-centric capacity building efforts (US

Department of State, 2024)—evinces a powerful state's efforts to establish an (informal) coalition of like-minded states in the governance of the digital environment.[74]

Could the (geopolitical) incentives for informal cooperation, then, have encouraged donors to invest more capacity building initiatives to encourage recipients' (geo)strategic alignment? Historically, the EU and the US have rejected formal UN treaties, preferring to retain the application of existing law onto cyberspace (Paulus, 2024). Arquilla (2021) argues that initially, Washington perceived the creation of formal treaties on cyberspace as potentially restricting its potential (future) operational and strategic advantages, including the possibility of offensive cyber capabilities. By contrast, China and Russia have advocated the importance of 'cyber sovereignty' and state-based control over internet content, infrastructure, and seek to secure a binding treaty—'primarily to constrain US and allied capabilities in this domain' (Sukumar et al., 2024, p. 14). Accordingly, the recent release of the UN Treaty on Cybercrime, initiated by Russia, potentially poses a further challenge to US and EU efforts to promote their historically preferred Budapest Convention on Cybercrime as the global model for cybercrime governance (which Russia has opposed). Given that this treaty covered only cybercrime, however vaguely defined, these developments may further incentivize the EU and the US to more actively promote their preferred approaches to other cybersecurity issues in informal settings, as a means of balancing against states which seek to pursue formally binding arrangements (such as Russia and China).

[74] Under the Biden Administration's approach, the government claimed to be 'rallying coalitions of governments, businesses, and civil society to shape the digital revolution at every level of the technology "stack" – from building subsea cables and telecommunication networks, to deploying cloud services and trustworthy artificial intelligence, to promoting rights-respecting data governance and norms of responsible state behavior,' (US Department of State, 2024, p. 4). Notably, while there have been stark cutbacks in USAID funding under the 2024 Trump Administration, the US State Department appears to have retained its *International Cyberspace & Digital Policy Strategy* of 'Building Digital Solidarity' (2024) from the Biden Administration, at least in name.

However, even for 'other-minded' states, such as China, and 'non-aligned' countries, as African countries have been recently characterized (Reddy, 2021), informal governance arrangements enable actors to engage in issue linkages, partake in forum shopping, and introduce new discussions on rules which might be curtailed in formal settings (Sukumar et al., 2024, p. 33). Indeed, as Chapter 4 demonstrated, capacity building instruments and approaches are not only confined to the West, but they have increasingly pervaded Chinese official discourses about digital development and cybersecurity. Indeed, the demand for digital development—and opportunities to supply capacity building assistance—have provided another forum for ideational and infrastructural competition. Given these wider developments, further research could valuable explore how and why capacity building assistance could contribute to the 'persistence of informality' in international cybersecurity governance (as put by Sukumar et al., 2024).

Separately, at the EU supranational level, this thesis focused upon several significant dimensions to the EU's contemporary geostrategic approach in and through cyberspace, as important pillars to the wider EU's strategic and foreign policy priorities in the 'Digital Decade' (Barrinha & Christou, 2022; Bellanova et al., 2022; Falkner et al., 2024). However, as EU external action policies towards cyberspace are transversal and continue to proliferate across a range of issue areas (Falkner et al., 2024), the EU's emerging actorness in cyberspace will continue to offer ripe opportunities for empirical studies regarding the drivers of EU policy changes in this field, perhaps by testing the drivers of change identified in Chapter 5 in new policy contexts. Several promising areas are in cloud computing, cyber/space integration, public-private partnerships for internal and external capacity building, and making digital infrastructure 'secure by design' in line with the EU's recent policies on *Cyber Resilience* and *Cyber Solidarity* (2024).

Regarding discursive change, further studies could examine in greater depth how varying national (territorial) approaches to sovereignty in and through cyberspace have implicated the formation of the EU's high-level geostrategic ambitions. Chapter 6 explored how, over time, vertical dissensus between Member States and EU supranational institutions gradually accommodated for an EU global role in and through cyberspace. EU institutions were able to make the case for EU involvement to EU constituents by linking the Union's empowerment to the cross-border, interdependent context of cybersecurity threats and their perceived relevance to the Union's capacity to function as a coherent political actor, suggesting that ontological security drives underpinning such spatial (b)ordering moves.

However, as Chapters 5 and 6 emphasized, European sovereigntist concepts have also been mobilized by both national governments (e.g Germany and France) and 'uploaded' to the supranational context to promote internal Europe coherence and cohesion vis-à-vis others and to diplomatically differentiate the Union's approach to global affairs from Washington (see also Csernatoni, 2022). These observations leave room for further examination of the national context, including relatively cyber mature countries with explicit yet distinct digital sovereignty mandates, such as Estonia, Germany, and France.

As Chapter 5 noted, the Council of the EU has been divided in terms of what 'European sovereignty' means to the EU's global positioning and ambitions: whereas some Member States understand it as a move towards protectionism and others have rejected this 'fortress Europe' conception and emphasized the importance of openness for European sovereignty. 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 *European* sovereignty and *EUropean* sovereignty. While the agent of sovereign control may be complementary across national and supranational bodies (Floridi, 2020), such contestation may also reflect, as Bickerton et al (2022) argue, vertical and horizontal

'sovereignty conflicts' between EU elites, and/or cross-national variation in public conceptions of 'sovereignty' as a concept (as discussed in Chapter 5). These ambiguities reflect the EU's longstanding entanglement with Westphalian and post-Westphalian concepts. Examining vertical contestation and Member States' domestic discursive environments in more depth would further contribute to our understanding about the EU's development as a coherent geostrategic actor. Below, I consider how the findings of the thesis relate to three general future trends and their implications for two further areas of research.

Wider trends and areas for research: the EU and geostrategic competition in an increasingly 'multipolar' digital age

This dissertation underscored the importance of the EU's relationships with other third countries in (re)constructing the Union's geostrategic approach and for pursuing the Union's geostrategic interests, including in the areas of cyber diplomacy and digital development. In particular, the chapters highlighted EU-US relations as a key factor in shaping the EU's global approach, both in terms of transatlantic cooperation (Chapters 5 and 6) and competition (Chapter 5) in various cyber-relevant policy areas. Strategic partnerships, as evidenced by the EU-US bilateral relationship, are both 'positional' in that they reinforce the EU's role and wider recognition as a global player and 'integrative' as they seek to ensure greater coherence between various EU actors in international affairs (Renard, 2018, p. 324). Moreover, they can be understood as relevant to Brussels' efforts to shape the global system, particularly in terms of fulfilling the Union's self-construction as the champion of multilateralism, the liberal order, and European values (Flockhart, 2020).

The increasingly fraught context of transatlantic relations, which have so far shaped the EU's geostrategic approach to cyberspace, may add further momentum to realizing the EU's emerging global strategic ambitions in the future. EU-US relations have been further

shaken by the inauguration of Donald Trump in January 2025, which were followed by several high-level instances of diplomatic disunity between European allies and Canada on the one hand, and the United States on the other. Following the 2025 Munich Security Conference, the Trump Administration's Secretary of Defence announced that the United States would no longer prioritize European security and that 'Europe was retreating from some of its most fundamental values […] shared with the USA' (quoted in Tidey, 2025). This may signal a 'paradigm shift' in transatlantic security cooperation, in which European strategic autonomy—and potentially digital sovereignty—becomes reality by dint of Washington's withdrawal from the continent (see also Bergmann, 2024). Several weeks later, President Trump and his vice President, JD Vance, publicly threatened Ukrainian President Volodymyr Zelenskyy that he was 'gambling with world war three' in a televised White House visit (Roth & Gambino, 2025).

Accordingly, the EU's role in European security, even within the context of cooperation in NATO, could become more prominent with the United States' potential pivot away from Euro-Atlantic security. After all, the early progenitors of today's European Union—the European Coal and Steel Community and the European Atomic Energy Community—were founded in 1951 in the wake of a bloody continental war. US withdrawal from European security, then, could inspire further strategic economic and security cooperation between European Member States, who have received come to regard the Union as a 'power multiplier' and the mouthpiece of European strategic autonomy and/or sovereignty concerns.

Nearly three years earlier, in March 2022, EU heads of state met 'informally' in Versailles to 'take further decisive steps towards building our European sovereignty' (European Council, 2022, p. 3). In what would become known as 'The Versailles Declaration', EU Member States pledged to reduce the Union's strategic dependencies

across several ‘sensitive areas’: critical raw materials, semi-conductors, digital, health, and food (European Council, 2022). The Declaration suggested that measures should be geared towards ‘maintaining [Europe’s] technological leadership*’* in semiconductors and ‘making Europe a leader’ in high technology sectors, such as biomedicine (European Council, 2022, pp. 7-8). Further, in 2023, the EU has put in place several recent cybersecurity acts which seek to concretize pan-European cybersecurity infrastructure and cooperation, including the *Cyber Resilience Act*, the *Cyber Solidarity Act*, and the *NIS2 Directive* (Farrand et al., 2024). Enhanced EU-led cooperation in (cyber) defence is suggested, for example, by recent calls by the Commission to activate the ‘escape clause’ in the Union’s fiscal rules to ‘substantially’ bolster Member States’ investment in defence through an EU defence framework (Tidey, 2025).

Equally, however, Trump’s approach to the Russia-Ukraine conflict may spur closer European *intergovernmental* cooperation, particularly between France, Germany, and the UK (no longer an EU Member State). Friedrich Merz, Germany’s next chancellor, recently expressed that, ‘My absolute priority will be to strengthen Europe as quickly as possible so that, step by step, we can really achieve independence from the USA’ (quoted in O’Donoghue, 2025)—but that does not mean that such cooperation will take place within the EU context. London’s widely speculated role as an emerging ‘bridge’ between the EU and the US not only underscores the longstanding importance of the UK in European security, but it may become the new fulcrum between two geostrategic blocs: the EU and the US. It is too early to tell whether the EU will provide an ‘integrated’ forum for European security and defence, in tandem with NATO, or if a British-led European security order will define future transatlantic relations (and by extension, the EU’s geostrategic ambitions), including in and through cyberspace. Regardless, these developments underscore the value

of gaining a deeper understanding of the EU's geostrategic ambitions and capacities as a global actor, including in the context of cyberspace.

A second general future trend concerns the relationship between private firms, state-based actors, and the digitalization of geostrategic competition. According to the leader of the EU's diplomatic branch, Josep Borrell, 'our future will be increasingly digital', so 'who will lead and set the rules in the digital domain is also a geo-political issue,' (European Union External Action Service, 2023). Thus, as he concluded in 2023, 'to be a rule setter, Europe *must indeed be a tech leader*,' (European Union External Action Service, 2023). Despite the EU's technological sovereignty ambitions, the thesis highlighted the significance of private actors in shaping dynamics of geopolitical competition in and through cyberspace. Briefly, Chapter 4 theorized that Washington, Beijing, and Brussels' relationships with private intermediaries was one key factor in mediating their choice of capacity building tools for pursuing geostrategic influence, alongside cultural and political variables. In turn, Chapters 5 and 6 highlighted the significance of European policymakers' concerns about dependence upon *foreign* suppliers (particularly the Chinese state-funded Huawei firm) in shifting Member States' perceptions that the EU could become a 'welcome player' in geostrategic discussions, paving the way for the popularization of European digital sovereignty discourse, as in the context of the 5G Toolbox.

These findings point to several areas for future research. First, reflecting the recent 'infrastructural turn' in IR (see Broeders et al., 2025), further studies could examine the nexus between state-private actor interactions and techno-geopolitical competition in the context of global digital infrastructure developments. In this vein, state-based actors have increasingly regarded the development, protection, and maintenance of undersea cables as a dimension of geopolitical competition and/or strategic escalation (McGeachy, 2021; Bueger & Liebetrau, 2021). Indeed, Chapter 4 examined EU, US, and Chinese efforts to compete in

providing and funding undersea cable projects that linked their respective geographies to African landing sites. However, in such consortia, there is a significant role played by global cable companies, as exemplified by China's state-funded firm, HMN Technologies, in constructing the PEACE Cable.

Government efforts to compete through digital infrastructuring practices may be further complicated by mounting efforts by global 'big tech' actors (e.g. Microsoft, Alphabet, and Amazon) to establish proprietary global digital infrastructure, including private undersea cable routes and cloud computing facilities. Whereas private sector involvement in undersea cables had been previously populated by 'highly specialized telecommunications companies', more recently, American big tech actors, particularly cloud service providers, have increasingly consolidated their influence over undersea cable developments (Bueger & Liebetrau, 2021, p. 405). Accordingly, changing configurations of the global internet backbone raise further questions about global power of big tech companies in mediating the dynamics of geostrategic competition. In future, countries along cable landing routes may be increasingly faced with a choice to opt for private or shared public-private cables, raising further questions about how countries perceive the geostrategic dimension to digital development. Further, these developments, including the resilience of global digital infrastructure, present further questions about the regulation of global data flows, having relevance for the EU's 'European digital sovereignty' and/or Russian and Chinese 'cyber sovereignty' regimes.

Given the EU's historical role as a liberal market actor and standard setter, the Union's relationship with both domestic and foreign firms in the 'Digital Decade' have emerged as a burgeoning area of research (see for example Farrand et al., 2024). This research has been important for underscoring the geoeconomic dimensions of the Union's strategic behaviour, although it has left room for making sense of how market logics have

been underpinned by the Union's ontological security drives and its spatial (b)ordering moves. This points to a fruitful avenue of further research.

Indeed, similar discursive moves detailed in Chapters 5 and 6 were employed in the European Commission's 2025 joint communication on 'Cable Security.' The Commission detailed its proposal to develop a 'Cable Security Toolbox', and 'to fund preparedness testing/stress testing of communication cables through the Cyber Solidarity Act' (2025, p. 5) in light of recent 'deliberate hostile acts' to undersea cables in the Baltic Sea (p.1). Recognizing the significant '*cross-border*' and 'economic relevance' of these cables, and the continent's reliance upon the infrastructure for 99% of its internet traffic, the Commission underscored the necessity of EU level action to protect the EU's strategic interests (p.1). There is ample room to further explore how the EU's efforts to spatially (b)order global digital networks have been shaped by its interactions with the private sector and its self-construction as a geostrategic actor. As geopolitical competition continues to unfold in and through cyberspace, EU spatial (b)ordering practices are likely to be a defining characteristic of the EU's external action beyond the current 'Digital Decade.'

Chapter conclusion

Geostrategic competition has emerged as a global development in and through cyberspace, generating imperatives for cyber-IR to make sense of its underlying foundations, drivers, and characteristics. This thesis has offered the first attempt to understand the co-constitution of cyber policies and geostrategic competition in the digital age from the perspective of the European Union's evolving external action approach. As I argued in this chapter, this study has laid the theoretical and empirical groundwork for developing an emerging framework on capacity-based foundations of cyber power, contributing to several important IR debates, and generated pathways for future research.

Conceivably, these research areas could be fruitfully examined by leveraging and refining the theoretical tools proposed earlier in this chapter. For example, a capacity-oriented approach can open up further opportunities for engagement with IR theories and/or insights which have remained on the margins of mainstream cyber-geopolitics research, including ontological security studies, as explored in Chapter 6. Equally, this approach has the potential to bring together largely siloed literatures relevant to cyber-IR. Examining capacity building assistance for digital development, as I explored in Chapter 4, provided a fruitful avenue to engage arguments in cybersecurity studies with scholarship in international political economy scholarship and security cooperation. Accordingly, a capacity-oriented approach could help to drive further theoretical innovation and/or knowledge creation in cyber-IR, including beyond this thesis. Future studies could examine the extent to which cyber and digital capacity have become fulcra for a government's capacity to project power within the context of rising private sector influence, shifting transatlantic relations, and a fragmenting multipolar global order pervaded by informal governance, strategic uncertainty, and digital interdependence.

Geostrategic behaviour in and through cyberspace have been characterized by evolving patterns of liminality and spatial (b)ordering. By mobilizing critical geopolitics, ontological (security), and capacity-oriented tools, we can better understand the constitutive ideas, institutions, and technologies which have made such dynamics 'virtually conceivable' in cyberspace. From a policy standpoint, this suggests that practitioners should consider a multidimensional perspective to cyber power: one which does not only privilege investment in cyber capabilities, but a capacity-oriented approach geared towards human expertise, strategic adaptation, and the ability to diffuse and integrate digital technologies into existing socio-technical infrastructures.

Chapter 7 References

Adams, P. C., & Warf, B. (1997). Introduction: Cyberspace and geographical space. *Geographical Review, 87*(2), 139–145. https://doi.org/10.1111/j.1931-0846.1997.tb00067.x.

Agnew, J. A. (2004). *Geopolitics: Re-visioning World Politics*. United Kingdom: Routledge.

Agnew, J., & Corbridge, S. (1995). *Mastering space: Hegemony, territory and international political economy*. Routledge.

African Union. (2020). *The digital transformation strategy for Africa* (2020–2030).

Arquila, J. (2021). *Bitskrieg. The new challenge off cyber warfare.* Polity Press.

Bacchi, C. L., & Goodwin, S. (2016). *Poststructural policy analysis: A guide to practice.* Palgrave MacMillan.

Backman, S. (2023). Risk vs. threat-based cybersecurity: the case of the EU. *European Security,* 32(1), 85–103. https://doi.org/10.1080/09662839.2022.2069464

Barrinha, A., & Christou, G. (2022). Speaking sovereignty: The EU in the cyber domain. *European Security,* 31(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895

Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines*. University of Michigan Press.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security, 3*1(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887.

Berenskoetter, F. (2017). Approaches to Concept Analysis. *Millennium: Journal of International Studies, 45*(2), 151-173. https://doi.org/10.1177/0305829816651934.

Bergmann, M. (2024, November 8). The United States now wants European strategic autonomy. *Center for Strategic and International Studies.* https://www.csis.org/analysis/united-states-now-wants-european-strategic-autonomy.

Bickerton, C., Brack, N., Coman, R., et al. (2022). Conflicts of sovereignty in contemporary Europe: A framework of analysis. *Comparative European Politics, 20*, 257–274. https://doi.org/10.1057/s41295-022-00269-6.

Borrell, J. (2023, June 27). Our stakes in digital diplomacy. European External Action Service. https://www.eeas.europa.eu/eeas/our-stakes-digital-diplomacy_en.

Borrell, J. (2024, September 26). *Op-ed by the High Representative/Vice-President Josep*

Borrell: The Draghi report and Europe's geopolitical future. European External Action Service. https://www.eeas.europa.eu/eeas/op-ed-high-representativevice-president-josep-borrell-draghi-report-and-europes-geopolitical-future_en.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology.* Oxford University Press.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization, 75*(1), 39–70. doi:10.1017/S002081832000051X.

Branch, J. (2024). Territory, sovereignty, and boundaries in digital battlespace. In T. Stevens & J. Devanny (Eds.), In *Research Handbook on Cyberwarfare* (pp. 301–315). Cheltenham, UK: Edward Elgar Publishing.

Bridges, L. E. (2024). Competing digital capacities: between state-led digital governance and local data center tradeoffs. *Information, Communication & Society, 27*(10), 1906–1923. https://doi.org/10.1080/1369118X.2024.2331765.

Broeders, D. (2007). The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants. *International Sociology, 22*(1), 71-92. https://doi.org/10.1177/0268580907070126.

Broeders, D., Sukumar, A., Kello, M., & Andersen, L. H. (2025). Digital corporate autonomy: geo-economics and corporate agency in conflict and competition. *Review of International Political Economy,* 1–25. https://doi.org/10.1080/09692290.2025.2468308.

Browning, C. S. (2018). Geostrategies, geopolitics and ontological security in the Eastern neighbourhood: The European Union and the 'new Cold War'. *Political Geography, 62*, 106-115. https://doi.org/10.1016/j.polgeo.2017.10.009.

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy, 42(*3), 391–413. https://doi.org/10.1080/13523260.2021.1907129.

Collett, R., & Barmpaliou, N. (2021). International cyber capacity building: Global trends and scenarios. *European Institute for Security Studies.* https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf.

Council of the European Union. (2021, February 3). Digital sovereignty is central to European strategic autonomy - Speech by President Charles Michel at "Masters of digital 2021" online event [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/.

Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European Security,* 31(3), 395–414. https://doi.org/10.1080/09662839.2022.2103370.

Ding, J. (2024). The rise and fall of technological leadership: General-purpose technology diffusion and economic power transitions. *International Studies Quarterly, 68*(2), sqae013. https://doi.org/10.1093/isq/sqae013.

Dodds, K., 2019. *Geopolitics: A Very Short Introduction*. Oxford University Press, Oxford.

Dunn Cavelty, M., & Wenger, A. (Eds.). (2022). *Cyber security politics: Socio-technological transformations and political fragmentation.* Routledge.

Drezner, D. W., Farrell, H., & Newman, A. L. (2021). *The uses and abuses of weaponized interdependence*. Brookings Institution Press.

Eberle, J., & Daniel, J. (2022). Anxiety geopolitics: Hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. *Political Geography, 92*, 102502. https://doi.org/10.1016/j.polgeo.2021.102502.

European Council. (2022, March 11). Informal meeting of the Heads of State or Government: Versailles Declaration, 10 and 11 March 2022. https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2025, February 21). Joint communication to the European Parliament and the Council: EU action plan on cable security (JOIN(2025) 9 final). https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables.

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty – Rhetoric and reality. *Journal of European Public Policy, 31*(8), 2099–2120. https://doi.org/10.1080/13501763.2024.2358984.

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs, 100*(6), 2379–2397. https://doi.org/10.1093/ia/iiae231.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351.

Flockhart, T. (2016). The problem of change in constructivist theory: Ontological security seeking and agent motivation. *Review of International Studies, 42*(5), 799–820. doi:10.1017/S026021051600019X.

Flockhart, T. (2020). Is this the end? Resilience, ontological security, and the crisis of the liberal international order. *Contemporary Security Policy, 41*(2), 215–240. https://doi.org/10.1080/13523260.2020.1723966.

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the

EU: towards digital sovereignty. *Journal of European Public Policy*, *31*(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology, 33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy, 45*(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062

Gerring, J. (2010). Causal Mechanisms: Yes, But…. *Comparative Political Studies*, 43(11), 1499-1526. https://doi.org/10.1177/0010414010376911.

Giddens, A. (2020). Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry (C. Hobbs, Ed.). *European Council on Foreign Relations*. https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/.

Gomez, M. A. (2019). Past behavior and future judgements: Seizing and freezing in response to cyber operations. *Journal of Cybersecurity, 5*(1), tyz012. https://doi.org/10.1093/cybsec/tyz012.

Hansen, L. (2006). *Security as practice: Discourse analysis and the Bosnian war.* Routledge.

Haroche, P. (2022). A 'geopolitical commission': Supranationalism meets global power competition. *JCMS: Journal of Common Market Studies, 61*(4), 970–987. https://doi.org/10.1111/jcms.13440.

Heidebrecht, S. (2024). From market liberalism to public intervention: Digital sovereignty and changing European Union digital single market governance. *JCMS: Journal of Common Market Studies, 62*, 205–223. https://doi.org/10.1111/jcms.13488.

Hix, S. (1994). The study of the European Community: The challenge to comparative politics. *West European Politics, 17*(1), 1–30. https://doi.org/10.1080/01402389408424999.

Hoffmann, S. (1996). Obstinate or obsolete? The fate of the nation-state and the case of Western Europe. *Daedalus, 95*(3), 862–915. https://www.jstor.org/stable/20027004.

Kinnvall, C., & Mitzen, J. (2020). Anxiety, fear, and ontological security in world politics: Thinking with and beyond Giddens. *International Theory, 12(*2), 240–256. https://doi.org/10.1017/S175297192000010X.

Klose, S. (2018). Theorizing the EU's actorness: Towards an interactionist role theory framework. *JCMS: Journal of Common Market Studies, 56*, 1144–1160. https://doi.org/10.1111/jcms.12725.

Klose, S. (2020). Interactionist role theory meets ontological security studies: an exploration

of synergies between socio-psychological approaches to the study of international relations. *European Journal of International Relations,* 26(3), 851-874. https://doi.org/10.1177/1354066119889401.

Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty.* Oxford University Press.

Krickel-Choi, N. C. (2021). *The embodied state: Why and how physical security matters for ontological security. Journal of International Relations and Development*, 25(1), 159–181. https://doi.org/10.1057/s41268-021-00219-x.

Krickel-Choi, N. C. (2022). State personhood and ontological security as a framework of existence: moving beyond identity, discovering sovereignty. *Cambridge Review of International Affairs*, 37(1), 3–21. https://doi.org/10.1080/09557571.2022.2108761.

Kuus, M. (2007). *Geopolitics reframed: Security and identity in Europe's eastern enlargement*. Palgrave Macmillan.

Lupovici, A. (2023). Ontological security, cyber technology, and states' responses. *European Journal of International Relations, 29*(1), 153-178. https://doi.org/10.1177/13540661221130958.

McCarthy, D. R. (2015). *Power, information technology, and international relations theory: The power and politics of US foreign policy and the internet*. London: Palgrave Macmillan.

McDermott, R. (2019). Some emotional considerations in cyber conflict. *Journal of Cyber Policy, 4*(3), 309–325. https://doi.org/10.1080/23738871.2019.1701692.

McGeachy, H. (2022). The changing strategic significance of submarine cables: old technology, new concerns. *Australian Journal of International Affairs, 76*(2), 161–177. http://dx.doi.org/10.1080/10357718.2022.2051427.

Microsoft. (February 4, 2025). Microsoft Cloud for Sovereignty. https://learn.microsoft.com/en-us/industry/sovereignty/sovereignty-capabilities.

Mitzen, J. (2018). Anxious community: EU as (in)security community. *European Security, 27(*3), 393–413. https://doi.org/10.1080/09662839.2018.1497985.

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security, 31*(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883.

Mügge, D. (2024). EU AI sovereignty: for whom, to what end, and to whose benefit? *Journal of European Public Policy, 31*(8), 2200–2225. https://doi.org/10.1080/13501763.2024.2318475.

Neumann, I. B. (1998). European Identity, EU Expansion, and the Integration/Exclusion Nexus. *Alternatives,* 23(3), 397-416. https://doi.org/10.1177/030437549802300305.

O'Donoghue, G. (2025, February 25). Macron walks tightrope with Trump as he makes Europe's case on Ukraine. *BBC News.* https://www.bbc.com/news/articles/cvg592557vgo.

Schmidt, V. (2011). Speaking of change: Why discourse is key to the dynamics of policy transformation. *Critical Policy Studies, 5*(2), 106–126. https://doi.org/10.1080/19460171.2011.576520.

Sjursen, H. (2011). Not so intergovernmental after all? On democracy and integration in European Foreign and Security Policy. *Journal of European Public Policy,* 18(8), 1078–1095. https://doi.org/10.1080/13501763.2011.615194.

Slayton, R. (2016). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. *International Security*, 41(3), 72–109. https://www.jstor.org/stable/26777791.

Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy,* 35(3), 468–486. https://doi.org/10.1080/13523260.2014.959261.

Smeets, M. (2022). *No shortcuts: Why states struggle to develop a military cyber-force.* Hurst Publishers.

Soifer, H., & vom Hau, M. (2008). Unpacking the strength of the state: The utility of state infrastructural power. *Studies in Comparative International Development, 43*(3), 219–230. https://doi.org/10.1007/s12116-008-9030-z.

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy, 45*(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739.

Radu, R. (2023). DNS4EU: a step change in the EU's strategic autonomy? *Journal of Cyber Policy, 8*(2), 239–256. https://doi.org/10.1080/23738871.2023.2295937.

Reddy, L. (2021). Is there space for a digital non-aligned movement? *Hague Centre for Strategic Studies.* https://hcss.nl/report/is-there-space-for-a-digital-non-aligned-movement/.

Renard, T. (2018). EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society, 19*(3), 321–337. https://doi.org/10.1080/23745118.2018.1430720.

Rone, J. (2024). 'The sovereign cloud' in Europe: diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. *Journal of European Public Policy, 31(*8), 2343–2369. https://doi.org/10.1080/13501763.2024.2348618.

Roth, A., & Gambino, L. (2025, March 1). Ukraine 'gambling with world war three',

Trump tells Zelenskyy in fiery meeting. *The Guardian.* https://www.theguardian.com/us-news/2025/feb/28/trump-zelenskyy-meeting-ukraine-aid-war.

Ten Oever, N., Perarnaud, C., Kristoff, J., Müller, M., Resing, M., Filasto, A., & Kanich, C. (2024). Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine. *Policy & Internet, 16*, 692–710. https://doi.org/10.1002/poi3.422.

Tidey, A. (2025, February 14). EU says Russia is the big threat, but US Vice President Vance disagrees. *Euronews.* https://www.euronews.com/my-europe/2025/02/14/in-munich-the-eu-seeks-common-ground-with-the-us-the-us-admonishes-the-eu.

US Department of State. (2024). United States International Cyberspace & Digital Policy Strategy. https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.

Weber, V. (2020). Making sense of technological spheres of influence. London: *LSE IDEAS.* https://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-Technological-Spheres-of-Influence.pdf.

Zarakol, A. (2017). States and ontological security: A historical rethinking. *Cooperation and Conflict, 52(*1), 48–68. https://www.jstor.org/stable/48512930.