(Re)bordering Europe in the Digital Decade: Mapping the EU's development as a global cyber actor

Julia Carver
DPhil Candidate, University of Oxford[1]
Dahrendorf Scholarship Essay, February 2025
Word count (excluding citations): 8908

Introduction

The global digital domain has emerged as a crucial space for geopolitical competition and the expression of territorial claims.[2] Indeed, the European context is no exception: the European Union's global approach to the digital domain has become a linchpin of its external action in a 'world of moving geopolitical plates.'[3] In such an environment, European policymakers have concluded that the Union 'must build its capacity to respond to evolving threats and its ability to act independently in the 'Digital Decade.'[4] Accordingly, under the current von der Leyen Commission, '*European digital sovereignty'* has become a central strategic objective for Brussels. Amidst fears that global interdependence has been weaponized,[5] such discourse issues a claim of legitimate authority over critical infrastructure and digital services within a particular functional and/or territorial jurisdiction.[6]

While scholars have keenly tracked developments in the EU's global cyber and/or digital policy, the significance of EU bordering practices—and territoriality—for shaping these policy shifts remains underexplored. This is a glaring gap for two reasons. First, at a basic level, claims to sovereignty and geopolitical goals are premised upon spatial (often geographically circumscribed) constructs with dual internal/external dimensions. Second, scholars have argued that bordering practices are foundational to upholding and/or reconstructing the EU's

---

[1] This essay adapts my doctoral research, part of which has been published in two research articles: see Julia Carver, "More bark than bite? European Digital Sovereignty Discourse and Changes to the European Union's External Relations Policy," *Journal of European Public Policy* 31 no. 8 (2024): 2250–86, doi:10.1080/13501763.2023.2295523; and Julia Carver, "Developing Digital "peripheries" for Strategic Advantage: Capacity Building Assistance and Strategic Competition in Africa," *Contemporary Security Policy* (2024): 1–42, doi:10.1080/13523260.2024.2430021. These articles are cited throughout the essay where relevant.

[2] Daniel Lambach, "The Territorialization of Cyberspace," *International Studies Review* 22 no.3 (2020): 482–506, https://doi.org/10.1093/isr/viz022.

[3] Council of the European Union, "A Strategic Compass for a stronger EU security and defence in the next decade," March 21, 2022, 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/; Sarah Bauerle Danzman, and Sophie Meunier, "The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator,"*JCMS: Journal of Common Market Studies*, 62 (2024): 1097–1115. https://doi.org/10.1111/jcms.13599.

[4] Council of the European Union, "Digital sovereignty is central to European strategic autonomy - Speech by President Charles Michel at 'Masters of digital 2021' online event," February 3, 2021. 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/; European Commission, "Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030," European Commission, *Strategic Foresight Report* [COM/2020/493 final], 2020.

[5] Daniel W. Drezner, Farrell, Henry, and Newman, Abraham L., eds., *The Uses and Abuses of Weaponized Interdependence* (Brookings Institution, 2021), https://www.brookings.edu/books/the-uses-and-abuses-of-weaponized-interdependence/.

[6] 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. Therefore, sovereignty is relational and socially constructed, with important material dimensions. See Sean Patrick Eudaily and Steve Smith, "Sovereign Geopolitics? Uncovering the 'Sovereignty Paradox," *Geopolitics* 13 no. 2 (2008): 309–34, doi:10.1080/14650040801991621; David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*.

identity and role in the world.[7] As Frank Schimmelfennig has argued, the process of delimiting and demarcating EU borders lies at the heart of the European integration project.[8]

Therefore, examining how particular EU bordering practices have constituted—and continue to shape—the Union's global approach to cyberspace would improve our understanding about the Europe's evolving role in the world. In the spirit of the Dahrendorf Programme's theme, *Europe in a changing world,* this essay asks: How has the EU engaged with bordering in cyberspace since its first cyber strategy, and what are the implications for the EU's role in the world? Drawing upon my doctoral research, this exploratory essay posits that the EU's approach to cyberspace has been characterized by three distinctive bordering practices over time: demarcation, externalisation, and (re)territorialization. Based on this exploration, I argue that the EU's evolving efforts to territorialize the digital domain seek to empower and reconstitute Europe's ('EUrope') position upon the contemporary geopolitical map. In so doing, such practices have (re)shaped opportunities for the Union enact its 'digital sovereignty' goals and for constructing the Union's role as a distinctly European global actor. However, they have also produced tensions with longstanding facets of the EU's self-representation as a global actor. In what follows, I elaborate my theoretical approach, key definitions, and empirical strategy. Next, I examine three developments in EU bordering practices vis-à-vis cyberspace, discuss their implications, and conclude with reflections about Europe in the (digital) world.

Bordering practices, sovereignty, geopolitics: a short review

Bordering practices, following Jordan Branch, are 'definitional' territorial practices, demarcating a particular relationship between space and power. [9] Such practices can have important political, social, economic, and security implications; their material and immaterial dimensions shape our world views and our understanding of belonging. After all, borders constitute an inside/outside demarcation between agents and/or spaces, serving as 'differentiating machines'[10] in a variety of institutional, ideational, and structural settings (as evidenced most prominently by immigration controls). They are inherently relational, differentiating between one's identity vis-à-vis others and the outside world.[11]

Bordering practices, Lambach argues, reveal how '[t]erritories are constituted through exercises of power and are also a source of power for whoever controls them.'[12] While borders can be 'fuzzy' and multilayered,[13] the boundary of a border nevertheless conveys aspects of 'closure' and 'control.'[14] Borders create closure through the establishment of inside/outside demarcations which often establish 'the exclusivity of rule' within the bordered space and/or territory, facilitating the political-legal basis for control.[15] Accordingly, sovereignty claims are considered inextricable with bordering practices, as 'the bordered territory has become the prevalent social form through which sovereignty is performed.'[16] Indeed, in the case of the EU,

---

[7] Schimmelfennig, 2021; Enrico Fassi, Michela Ceccorulli, Sonia Lucarelli, "An illiberal power? EU bordering practices and the liberal international order," *International Affairs 99* no. 6 (2023): https://doi.org/10.1093/ia/iiad228.
[8] Schimmelfennig, 2021.
[9] Branch, 2017 p. 137.
[10] Jussi P. Laine, "Ambiguous bordering practices at the EU's edges," in Andreanne Bissonnette and Élisabeth Vallet (Eds.) *Borders and Border Walls: In-Security, Symbolism, Vulnerabilities* (Routledge, 2020). Quoting Enrica Rigo, *Europa di Confine. Trasformazioni Della Cittadinanza Nell'unione Allargata. Rome: Meltemi editore*, 2007.
[11] Laine, 2023.
[12] Lambach,2020, p. 488..
[13] Jan Zielonka, *Europe as Empire: The Nature of the Enlarged European Unio*n (Oxford, 2006).
[14] Schimmelfennig 2021.
[15] Jordan Branch, "Territory as an institution: spatial ideas, practices andtechnologies," *Territory, Politics, Governance 5* no. 2 (2017): 137, http://dx.doi.org/10.1080/21622671.2016.1265464.
[16] Kristine Beurskens and Judith Miggelbrink, "Special Section Introduction – Sovereignty Contested: Theory and Practice in Borderlands," *Geopolitics* 22 no. 4 (2017): 750, https://doi.org/10.1080/14650045.2017.1373582.

Benjamin Farrand and Helena Carrapico argue that 'Digital sovereignty is […] a call for a reassertion of the EU's technological independence, a desire to "take back control" of the governance of cyberspace and an assertion of its willingness to protect its digital borders from outside competition.'[17]

However, in the case of the EU, control—including the capacity to enforce borders—is mediated by both the member state and supranational competencies and capabilities.[18] European 'bordering' practices have therefore been credited as shaping the Union's consolidation as a political actor and in managing recent crises, such as the 2015 migration crisis.[19] For example, EU has been held to export Europeanizing practices to its 'borderlands'—or those neighbouring states without a membership perspective—in order to 'stabilize' its external Neighbourhood.[20] Prospective EU member states also have a complex relationship to EU borders, as they are seen as 'outside' of the Eurozone yet associated to the Union through various candidacy processes.[21] These dynamics, according to Schimmelfennig, evince how EU bordering practices undergird European integration processes.[22]

Therefore, EU bordering practices in cyberspace have been equivocated by scholarship emphasizing the dual dimension to European digital sovereignty: first, as a claim to legitimate control over the Union's *internal* digital environment (e.g. the 'Digital Single Market') and second, a claim to shaping its own destiny in the (external) global digital domain.[23] At the same time, scholars have also demonstrated that sovereigntist claims in and through cyberspace are often practically overlapping or 'pooled' with other political entities, including nation states and private actors.[24]

EU bordering practices vis-à-vis the digital domain are further complicated by the structural characteristics of cyberspace and global digital interdependence. Cyberspace challenges classical assumptions about international relations, whereby the state, sovereignty, and the military are territorially packaged into 'a bordered power container.'[25] With a fluid, complex, and tenuous link with physical geography, cyberspace tends to 'represent a threat to the spatialized forms of intelligibility and control'[26] by challenging the so-called

---

[17] Benjamin Farrand & Helena Carrapico, "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity," *European Security*, 31 no. 3(2021): 435–453. https://doi.org/10.1080/09662839.2022.2102896.

[18] Schimmelfennig 2021.

[19] Anssi Paasi, "Examining the persistence of bounded spaces: remarks on regions, territories, and the practices of bordering, " *Geografiska Annaler: Series B, Human Geography*, *104* no. 1(2022): 9–26. https://doi.org/10.1080/04353684.2021.2023320.

[20] Raffaella Del Sarto, "Normative Empire Europe: The European Union, its Borderlands, and the 'Arab Spring'" *Journal of Common Market Studies* 54 no. 2 (2015): 215-232, https://doi.org/10.1111/jcms.12282; see also Jan Zielonka, 2006.

[21] Tina Freyburg and Solveig Richter, "National identity matters: the limited impact of EU political conditionality in the Western Balkans," *Journal of European Public Policy*, *17* no. 2(2010): 263–281. https://doi.org/10.1080/13501760903561450.

[22] Schimmelfennig, 2021.

[23] Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." For broader work on sovereignty, see Janice Thomson, "State Sovereignty in International Relations: Bridging the Gap between Theory and Empirical Research," *International Studies Quarterly* 39, no. 2 (1995): 213-233, https://doi.org/10.2307/2600847; Julia Pohle and Thorsten Thiel, "Digital Sovereignty," *Internet Policy Review* 9, no. 4 (2020): 1–19, https://doi.org/10.14763/2020.4.1532.

[24] See Lambach, 2020.

[25] Anthony Giddens, *The Nation State and Violence: Volume Two of A Contemporary Critique of Historical Materialism* (Cambridge: Polity, 1985); Thierry Balzacq and Myriam Dunn Cavelty, "A Theory of Actor-Network for Cyber-Security," European Journal of International Security 1, no. 2 (2016): 186, https://doi.org/10.1017/eis.2016.8.

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

'Westphalian'[27] contiguity between (nation-state) sovereign authority.[28] Promising low entry barriers and a networked architecture transcendent of state boundaries, cyberspace had seemed to introduce a world of emancipation from state control.[29] However, fears about the 'Balkanization of the internet' and cyber- 'spheres of influence' eschew this optimism.[30]

Furthermore, there is an indelible geographic component to cyberspace; its physical backbone (comprised of undersea cables, satellites and other critical digital infrastructure) enables global connectivity, facilitates information flows, and the establishment of a virtual (cyber)space. Control over grounded digital infrastructures, then, can enable governments to 'territorialize' certain parts of a global network by creating 'spatial fixes' through erecting nodal connections in physical space.[31] Equally, accessing 'remote' or space-based infrastructures such as satellites can enable global actors to overcome geographic limitations and compete over cyberspace.[32] Thus, as Myriam Dunn Cavelty and Thierry Balzacq have argued, cyberspace does not constitute a 'clean break' from Westphalian traditional actors and institutions, but it equally cannot be essentialized into a post-Westphalian geographical space.[33] Arguably, these tensions are not unlike the EU's own relationship to borders: the Union is not comprised by a straightforward 'state-force-territory' relation.[34] Rather, sovereignty claims uttered by the EU are the product of a complex interweaving of different intergovernmental and supranational competences.[35] Consequently, EU bordering practices, are inherently dialectical, characterized by overlapping and non-exclusive territorial boundaries alongside those of EU Member States.[36]

Beyond the material, the EU's embrace of 'European digital sovereignty' discourse and a 'geopolitical approach' can be seen to draw upon geographically defined imaginaries of Europe in the world.[37] As Eberle and Daniel argue, international politics may also be 'spatialised' through the production of 'geopolitical imaginations' by engaging actors at the

---

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

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

[29]John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation,* 1999, https://www.eff.org/cyberspace-independence; see also or instance, refer to Georgios I. Zekos, "Demolishing State's Sole Power over Sovereignty and Territory Via Electronic Technology and Cyberspace.," *Journal of Internet Law* 17, no. 5 (2013): 3–17, http://proxy.lib.sfu.ca/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=91743838&site=ehost-live.

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

[31] Colin Turner and Debra Johnson, "Infrastructure and Territoriality," *in Global Infrastructure Networks: The Trans-national Strategy and Policy Interface* (Cheltenham, UK: Edward Elgar Publishing, 2017); Julia Pohle and Daniel Voelsen, "Centrality and Power. The Struggle over the Techno-Political Configuration of the Internet and the Global Digital Order" *Policy & Internet* 14, no. 1 (2022): 13–27, https://doi.org/10.1002/poi3.296..

[32] Mia M. Bennett and Trym Eiterjord, "Remote control? Chinese satellite infrastructure in and above the Arctic global commons," *The Geographical Journal* (2022) 1– 14. https://doi.org/10.1111/geoj.12503.

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

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

[35] Stefano Bartolini, *Restructuring Europe: Centre Formation, System Building, and Political Structuring between the Nation State and the European Union* (Oxford Scholarship Online, 2006).

[36] Barrie Axford, "The Dialectic of Borders and Networks in Europe: Reviewing 'Topological Presuppositions," *Comparative European Politics* 4 (2006): 160–182.

[37] N.B. These imaginaries need not be defined in terms of the nation state, but they nevertheless have a geographic or spatial character by definition. See Jussi Laine, 2022.

affective level.[38] While 'digital sovereignty' implies the existence of a bounded European sociotechnical space(s) to be controlled, Brussels' 'geopolitical approach to cyberspace' suggests a desire to project power in the digital domain through competitive structural positioning.[39] However, we lack an understanding about how such an imaginary has been developed and reinforced by EU bordering practices in and through the digital domain over time.[40]

This paper seeks to illuminate these issues by drawing upon aspects of my doctoral research through the lens of bordering practices. I approach bordering practices through an exploratory perspective, seeking to foreground how EU discourses and policies establish internal/external demarcations in and through cyberspace. This enables me to explore how the EU's external action has constructed a constitutive European 'inside' versus a non-European 'outside' in both the material (e.g. structural/physical/functional) and immaterial (social/relational) aspects of the digital domain. Conceptually, I adopt a critical geopolitics approach to territoriality as entailing both material (technological, geographic) and immaterial (ideational) aspects.[41] This approach is further outlined below.

Approaching EU bordering in and through cyberspace: discourses, practices, and context

In this short paper, I focus upon the discourses and practices[42] in relevant EU institutional contexts which comprise EU bordering *in and through* cyberspace in the context of external action. In line with my interpretive-qualitative approach, I conceive of cyberspace and the digital domain as subjective, socio-technical spaces *as they have been defined by the actors themselves*.[43] Not only has the EU has increasingly framed cyberspace (and the digital domain) as an interconnected, integrated aspect of EU external action, but it has become understood as a defining feature of the contemporary global world. As underscored by the COVID-19 pandemic, the world has seen an increased 'hybridization' of digital ('the virtual') and physical ('the real') spaces; a blurring of online and offline spaces.[44] Cyberspace is therefore not only a 'separate sphere, but part of the lived experience of people.'[45]

Currently, the EU generally conceives of cyberspace as the 'fifth domain of warfare' and as an overlapping environment to the digital domain (whereby the latter is more encompassing and encapsulates policy areas, such as semiconductors and cloud computing).[46] Thus, the framing '*in and through cyberspace'* speaks to the analysis undertaking broader approach outlined above: I will be exploring EU bordering practices which have engaged cyber issues (including discourses and policy instruments) to demarcate political space relevant to

---

[38] Eberle and Daniel, 2022: Anxiety geopolitics: hybrid warfare, civilisational geopolitics, and the Janus-faced politics of anxiety. Political geography, 92, 102502.
[39] Ibid.
[40] This is suggested by Csernatoni (2023) but not examined in any depth over preceding periods to the von der Leyen Commission. See Raluca Csernatoni, "The EU's Hegemonic Imaginaries: From European Strategic Autonomy in Defence to Technological Sovereignty," *European Security* 31 no. 3 (2022): 395–414, https://doi.org/10.1080/09662839.2022.2103370.
[41] Drawing upon Branch (2017).
[42] By focusing upon EU policy discursive contexts, this study undertakes an 'inside-out' approach to exploring EU bordering practices. A valuable extension to this research would be to examine how 'outsiders' (non-EU actors) have discursively constructed the EU, to explore more thoroughly how social recognition and interaction with the EU's 'constitutive outside' informs its own bordering practices. Promising empirical cases would include the recipients of the EU's cyber partnership funding (countries in its Southern and Eastern Neighbourhoods), for example, or key EU allies and rivals (the US and China, respectively).
[43] John Agnew and Stuart Corbridge, *Mastering Space: Hegemony, Territory and International Political Economy* (London: Routledge, 1995).
[44] Lambach, 2020.
[45] Cohen 2007, p. 2010, in Lambach, 2020.
[46] See Carver, 'More bark than bite?', 2024.

the Union's global approach to the digital domain. Consequently, the analysis in this short paper is not exhaustive. However, by focusing upon EU bordering practices in the context of the EU's evolving cyber strategy, this study advances an emerging research agenda in EU cyber studies focusing upon bordering practices and their relationship to the EU's development as a global actor in the 'Digital Decade'.

Overview of methodology

As mentioned above, the substantive basis of this essay is drawn from this author's doctoral research,[47] based upon an interpretive-qualitative analysis of primary source documents and 25 elite interviews,[48] and by drawing upon extant scholarship in the fields of EU studies, international relations, and public policy. Archival documents and primary sources over the 2006-2024 timeframe, largely drawn from the EURLEX database, comprised the main primary source material. This timeframe encapsulates the release of the EU's first ever cybersecurity strategy, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013); the highly influential *Global Strategy for the European Union* (2016), the 2017 updated cybersecurity strategy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* (2017), 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 in external action, viz. the EU's *Strategic Compass* (2022) and internal cybersecurity, viz. the *NIS2 Directive* (2023) amongst others.

Within this timeframe, I identified relevant sites of analysis through a temporalized mapping technique, which traces and situates the ideational positions of actors located in different policy settings.[49] Together with the interview data, this chronological mapping process facilitated further exposure to the perspectives of the multitude of agents involved in shaping and disseminating EU cybersecurity discourse.[50] Notably, the EU has increasingly integrated cybersecurity instruments into its external action outlook over time, including in the CDSP/ESDP area. This is apparent by comparing the EU's first cybersecurity strategy to the contemporary 2020 version (as presented in Figures 1 and 2 below).

---

[47] Part of which has been published: See Carver, 'More bark than bite?', 2024; 'Developing digital peripheries for strategic advantage', 2024. I would like to gratefully acknowledge Nuffield College and the Economic and Research Council for funding my research [ES/P000649/1].

[48] See Carver, 'More bark than bite?' 2024, pp. 2257-59. 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.

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

[50] Clarke, Friese, and Washburn; Schwartz-Shea and Yanow, *Interpretive Design: Concepts and Processes.*

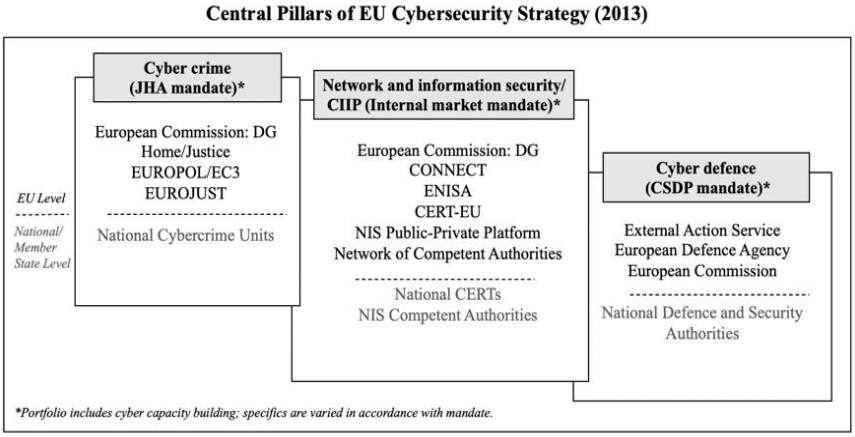

Figure 1. Central pillars of EU cybersecurity strategy (2013), as compiled by George Christou.[51] *Diagram here was reproduced, with slight modifications, by the author.*

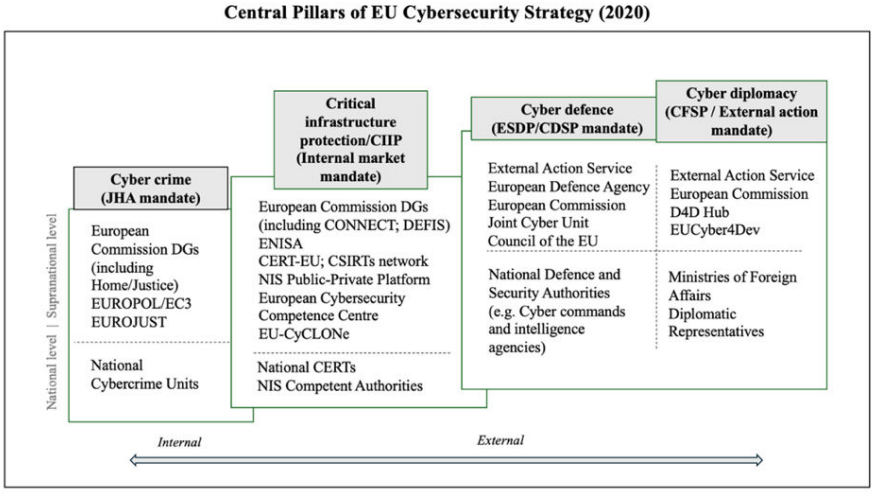

Figure 2. Central pillars of the EU's 2020 cybersecurity strategy (in force) and relevant institutional actors, compiled on the basis of the author's institutional mapping and updated for 2020 in line with the European Parliamentary staff document.[52]

In line with the EU's legal and political competences towards cyberspace, this essay approaches EU external action policy as a process that is shaped 'with reference to values and principles that are seen as *particular* to the Union.'[53] Such an approach, which supersedes pure intergovernmentalism, captures the bulk of developments in EU cyber and digital policy post-Lisbon Treaty in the domain of external action.[54] EU external action policymaking is also

[51] See George Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, ed. Stuart Croft, *New Security Challenges Series* (Hampshire: Palgrave MacMillan, 2016).

[52] Polona Car, "Cybersecurity actors in the EU," *European Parliamentary Research Service,* 2024, https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757594/EPRS_ATA(2024)757594_EN.pdf.

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

[54] Moritz Laurer and Timo Seidl, "Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation," *Policy and Internet* 13, no. 2 (2021): 257–77, https://doi.org/10.1002/poi3.246; Paul Timmers, "The European Union's Cybersecurity Industrial Policy," J*ournal of Cyber Policy* 3, no. 3 (2018): 363–84, Patryk Pawlak, *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building*; Panagiotis Trimintzios et al., "Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and Risks for the EU" (Brussels, 2017), p. 5.

shaped by internal cohesion (as defined by policy coordination, including between Member States, and the coherence of concepts across different policy areas); international recognition; and structural conditions imposed by the EU's surrounding global environment.[55]

The ensuing analysis is organized around the release and formation of the Union's 2013, 2017, and 2020 official cyber strategies, which coincide with three important phases in the EU's development as a global cyber actor.[56] While space constraints dictate the brevity of this essay's coverage of EU cybersecurity policy developments and drivers, it should be emphasized that the development of EU external action policies and debates about cybersecurity have multiple causal drivers, institutional path dependencies, uneven EU competences across policy areas, exogenous events, and varying strategic goals of policy elites.[57] To recapitulate, the aim of this paper is not to generate exhaustive conclusions regarding the future of the EU's global approach to cyberspace or complete causal explanations for its contemporary outlook. Rather, I intend to highlight a significant yet overlooked dimension to the EU's evolution as a global actor: its engagement with bordering practices and territoriality in and through cyberspace. I subsequently discuss the implications of these findings for the EU's position in a changing world and its geopolitical goals.

Bordering practices and the EU's development as a global cyber actor in a changing world

The last eleven years have seen significant developments in the European Union's cybersecurity policies and its global approach in the digital age. The EU's first *Cybersecurity Strategy* in 2013 advanced a modest, inward-looking approach to cybersecurity which remained largely agnostic of its fit within the EU's external relations approach. Seven years later, Brussels released its updated strategy, which asserted the goal to achieve '*European technological sovereignty*' in the 'Digital Decade.' [58] Below, I review several key EU cyber-external action policy developments which serve to demarcate, reinforce, and (re)construct the EU's position in global cyberspace.

As I review in this section, European debates surrounding the meaning(s) of cyberspace prior to the 2010s reveal discursive struggles to define and demarcate space in the cyber environment, and by extension, the EU's role as an actor. During this period, the EU's bordering practices were largely inward-looking, with respect to how the EU's authority over cyberspace would be demarcated vis-à-vis its Member States. Subsequently, the 2017 cyber strategy update emblematized the EU's turn to externalising threats in the cyber environment to bolster its internal security and construct the Union as a 'secure' (cyber)space. Finally, the 2020 cyber strategy was shaped by the EU's new 'geopolitical' approach to border management in and through cyberspace. Additionally, it debuted sovereigntist claims vis-à-vis digital technologies and the European 'digital domain' as an aspect of the EU's strategic outlook towards global cyberspace.

---

[55] Stephan Klose, "Theorizing the EU's Actorness: Towards an Interactionist Role Theory Framework,"*JCMS* (2018) 1144, https://doi.org/10.1111/jcms.12725.

[56] See also Helena Carrapico and Benjamin Farrand, "Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics," *JCMS* (2024): https://doi.org/10.1111/jcms.13654.

[57] See for instance Carver 2024, 'More bark than bite?'.

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

2007-2013: *Demarcating* European cyberspace

The development of the EU's first cybersecurity strategy, and thereby the securitization of cyberspace as an EU policy field,[59] has been characterized by multifaceted and overlapping 'bordering' practices. Prior to the mid-2000s, issues in cyberspace were not viewed as key challenges to the EU's security.[60] However, the 2007 cyberattacks targeted against Estonian critical infrastructures were a triggering event for the securitization of cyberspace in the EU policy context.[61] Afterward, European policy discourses shifted from an emphasis on *computer-* or *information security* to *cybersecurity.* Whereas the former focused upon *technical* discourses in the context of computer science, the latter marked a turn to incorporating 'cyber' into the 'specialized arena of [trans]national security.'[62]

Notably, European policymakers' responses to the Estonia cyberattacks were concentrated within disparate strategic communities at the Member State/national level[63] as opposed to EU-level policy discourse.[64] For some Member States, particularly Estonia, the attacks reinforced their concerns about the connection between cyber threats and the broader geopolitical tensions in the EU's neighbourhood.[65] Indeed, the Estonian government stated that these cyberattacks were 'a blatant attack not only on Estonia's sovereignty, but also on the entire European Union.'[66] Reflecting upon the attacks, a French government official remarked, 'It thus appears necessary for states to plant the flag in the spaces they occupy in order to exercise all their sovereign functions, colonize virgin spaces, and be prepared to confront adversaries in this [cyber]space'.[67] Such discourse invokes a clear territorial representation of cyberspace through a nation-state framework.

By 2010, 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. For example, the British government's skepticism about whether it was 'sensible to develop European-centric approaches at all,' is illustrated by the following statement during a parliamentary debate in 2010:

> '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.' [68]

This vision confines the scope of EU action in cyberspace to internal *European* matters and discourages the EU's involvement (as the embodiment of the European-centric approach) in

---

[59] For further reference, see George Christou, "The Collective Securitisation of Cyberspace in the European Union," *West European Politics* 42, no. 2 (February 23, 2019): 278–301, https://doi.org/10.1080/01402382.2018.1510195.

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

[61] Other significant events during this time period were Stuxnet (2010), a malware attack on Iranian centrifuges, and the Snowden leaks in 2013 (highlighting government cyber surveillance by NSA and GCHQ), amongst others.

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

[63] Interviewee B, interview by author, virtual (online video), March 11, 2021; in Carver, 2024, 'More bark than bite?'.

[64] This is partly due to the EU's institutional competences and lack of foreign policy mandate. Prior to the enactment of the Lisbon Treaty in 2009 and the inception of the EU External Action Service (EEAS) in 2010, the EU had few foreign and security competencies necessary for its empowerment to act on behalf of its Member States, and there was no clear mechanism at the EU level to produce a foreign policy response.

[65] Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee F, interview by author, virtual (online video), April 15, 2021; in Carver, 2024, 'More bark than bite?'.

[66] NATO CCDOE, "2007 Cyber Attacks on Estonia", 56.

[67] Stéphane Dossé, cited in Frédérick Douzet, "Understanding Cyberspace with Geopolitics," *Hérodote* 1, no. 152–153 (2014): 3–21.

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

global cyberspace or matters of security. The UK justified this position on the grounds that 'the Internet operates as a global phenomenon and *does not recognise borders*,'—therefore, cyberspace does not warrant a European-centric focus. [69] According to the UK's position, the lack of borders in cyberspace implies there is no *global European (cyber)space*—and therefore no grounds for a broader EU role.

An EU Commissioner vehemently rebutted this position, arguing that without EU involvement, 'there is no possibility for Europe as a region to cope, to work in the globalised environment of electronic communication networks and services unless there is first a kind of unified way of approaching the problem.'[70] Consequently, the Commissioner sought to establish construct cyberspace through a regional perspective, thereby demarcating European borders in the 'globalized' environment as a necessity for Europe's capacity to cope with cyber issues. 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.

Debating a collective European approach to a policy domain is not novel from the perspective of European integration (such as the British position above). However, cyberspace remains distinctive in terms of the level of conceptual and ontological disagreement it elicited for EU policymakers.[71] A 2009 report published by the EU's General Secretariat noted the lack of shared agreement on what constituted cyberspace—let alone cybersecurity—amongst EU policymakers and reiterated the need to establish a formal definition.[72]

This is further illustrated by the proliferation of bordering discourse in debates at the horizontal (supranational) level. During this period, 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.'[73] Such an account envisioned European states' territorial sovereignty, and their role as security providers, as neatly mapped onto cyberspace. Thus, while the Council expected cybersecurity challenges to cross the internal/external dimensions and pillars of the EU due to its cross-border nature,[74] it believed that cyberspace did not bring about the dissolution of boundaries on the whole.

The Council's position contrasted starkly with the view promulgated by the European Organization of Security (EOS) working group, which engaged with Brussels in a stakeholder capacity and represented the view of academic experts and European private companies. To establish the 'scope' of the problem, a 2010 European Organization for Security (EOS) White Paper conceived of 'the cyberspace' as distinct from 'the real world' (2010), thus embedding a sense of unreality to the meaning of cyberspace.[75] Given that geopolitical activities are firmly grounded in the 'real (physical) world', it can be inferred that, for the authors of this document, geopolitical logics did not serve as the prominent conceptual 'coordinates' through which to make sense of cyberspace.

Comparing these approaches to that of a third policy community—the EU Commission—reveals further ontological dissonance about the spatial character of cyberspace, and a somewhat piecemeal aggregation of the above two views. This conception is clearly articulated in the 2010 *Digital Agenda for Europe,* of which it was the penholder. The document describes cyberspace as a 'borderless' domain, advancing the argument that online barriers to markets should accordingly be struck down. However, it also recognized the strategic importance of the internet and the necessity for including an *external dimension* to cybersecurity to preserve a

---

[69] Emphasis added by author. European Union Committee.
[70] European Union Committee.
[71] By comparison, few EU officials would disagree about the *fundamental* nature of 'sea' or 'air' as strategic domains.
[72] Jean-Pascal Zanders, "Cyber Security: What Role for CFSP?," *European Union Institute for Security Studies* (Brussels, 2009).
[73] Zanders, "Cyber Security: What Role for CFSP?", 2.
[74] Zanders.
[75] European Organisation for Security, 'Towards a concerted EU approach to cyber security', September 2010.

'European digital way of life.' This secondary provision reproduces the Council's notion that Europe should protect the part of cyberspace for which it is responsible, although from a 'European' (not state-centric) standpoint. Hence, the EU's imaginary of borders is reproduced: a harder external (non-European) border yet lowered barriers in the context of the EU's internal market.

By 2013, the release of the EU's first cybersecurity strategy laid the essential foundations for a collective European approach. While the strategy was a combined effort from then-Home Commissioner Cecilia Malmström, High-Representative Catherine Ashton, and DG Connect Commissioner Neelie Kroes—thus incorporating both the external and internal aspects of the EU's competence in cybersecurity—the focus of the policy was largely inward-looking. Indeed, the EU's role was clearly circumscribed to internal EU matters, and issues within extant EU borders and competences, prioritizing the protection of critical infrastructure within the internal market and the network and information security of European essential services.[76] At this point, for skeptics such as the UK, the EU's collective approach was permitted as '[The] relatively recent shift towards greater dependency and reliance on internet based systems and networks across Europe means a change in the approach […] that recognises that cyber related risks and attacks could now impact and affect more than just one nation.'[77] This orientation served the purpose of reaffirming the EU's *historically established* role as an economic security provider for EU citizens (and Member States), thereby demarcating an EU territorial role which aligned with its responsibilities as a European economic security provider.

Notably, the *specificities* of the EU's role vis-à-vis cyberspace were left equivocal in this strategy due to competing visions about the EU's role as an actor beyond reinforcing its existing prerogatives (and competences) towards the Internal Market. The document emphasized that, due to the leading role of the private sector and the 'diverse range of actors involved, *centralised, European supervision is not the answer*.'[78] Nevertheless, while recognizing that Member States governments had significant roles to play, it stated that 'an effective national response would often require EU-level involvement.' [79] Altogether, the document evinced the lack of 'collective vision' about cybersecurity at the EU level during this period.[80]

Dissensus over a European cyber 'space' and the invisibility of geopolitics

The 2013 strategy reflected enduring dissensus surrounding the global nature of the EU's role in cyberspace and its involvement in issues traditionally associated with national security (including geopolitical issues), prescribing a relatively vague and reactive role for the EU in cyberspace. Moreover, it was emblematic of how geopolitical concepts remained delegitimized in official EU discourse: despite advancing an overly inclusive conceptualization of the origins of security threats in cyberspace, Europe-wide geopolitical motives or tactics were notably absent from this list.

Compared to the issues of cyberattacks and cybercrime, geopolitical issues were scarcely discussed in *public* EU diplomatic settings during the 2009-2013 period.[81] Moreover, when such issues were discussed within the Commission and the EEAS, there was no clear agreement

---

[76] European Commission and High Representative of the Union for Foreign Affairs and Security Policy.
[77] European Union Committee, 50, emphasis added.
[78] Emphasis added by author. European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 17.
[79] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 17.
[80] Helena Carrapico and André Barrinha, "The EU as a Coherent (Cyber)Security Actor?" *Journal of Common Market Studies* 55, no. 6 (2017): 1254–72, https://doi.org/10.1111/jcms.12575.
Barrinha, "The EU as a Coherent (Cyber)Security Actor?"
[81] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; in Carver, 2024, 'More bark than bite?'.

as to how the cyber environment could be geopolitical.[82] Subtle references to geopolitical concepts in official documents—if at all present—were vague and contradictory. For example, the Commission's *Digital Agenda for Europe* (2010) affirmed that 'the digital age is neither "big brother" nor "cyber wild west".[83] Yet, a Commission Communication on *Critical Information Infrastructure Protection* (2011) published shortly thereafter noted that the:

> 'global geo-political dimension [of new technological threats] is becoming progressively clearer. We are witnessing a trend towards using ICT [information and communications technology] for political, economic and military predominance, including through offensive capabilities.'[84]

These constructions elicit a contradictory image of cyberspace: whereas the first description offered a comparatively more reassuring, non-conflictual conception of security in a digitalized world (through its assurance that cyberspace was *not* a cyber wild west), the second text stressed the increased geopolitical dimension to 'new technological threats', invoking a framing of the cyber environment often articulated by 'Digital/Cyber Wild West' discourses elsewhere.[85]

Thus, while this brief analysis only offers a slice of many different bordering perspectives in the EU policy context, it is apparent that the 'borderless' nature of cyberspace presented both a problem and an opportunity for EU policy actors to reconstruct the EU's reach and authority as a cyber actor. Defining the scope and capabilities of the EU's approach to global cyberspace was evidently shaped by the preferences of different policy actors across different EU institutional contexts. Meanwhile, EU internal dissensus stymied coherent geopolitical constructions of cyberspace at the EU level.

2014-2017: *Externalising* EU cyber insecurities through bordering

The 2014 Ukraine crisis (which included cyber operations), the 2015 migration crisis, and the 2016 election of Donald Trump constituted significant 'wake-up calls' for European policymakers regarding the EU's security environment, stoking the impression that the Union was surrounded by a 'ring of fire.'[86] Particularly, the 2014 Ukraine crisis reinforced that cyberspace could be used to threaten the EU's geographical environment; the EEAS surmised that Russian hybrid warfare had 'compromised Ukraine's territorial integrity and […] strived to destabilise the larger neighbourhood'.[87] Similarly, a 2015 European Parliament paper attributed the emergence of hybrid cyber operations to the 'changing global environment', citing Russian and Chinese state-backed hacking as prime examples.[88] During this period,

---

[82] Interviewee A, interview by author, virtual (online video), March 5, 2021; in Carver, 2024, 'More bark than bite?'.
[83] European Commission, *A Digital Agenda for Europe Communication 5 No. 245 final/2,* Brussels 2010, 16, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.
[84] European Commisssion, *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection 'Achievements and next Steps: Towards Global Cyber-Sec*, Brussels, 2011, 3, http://publications.lib.chalmers.se/records/fulltext/245180/245180.pdf%0Ahttps://hdl.handle.net/20.500.12380/245180%0Ahttp://dx.doi.org/10.1016/j.jsames.2011.03.003%0Ahttps://doi.org/10.1016/j.gr.2017.08.001%0Ahttp://dx.doi.org/10.1016/j.precamres.2014.12.
[85] As a competitive, power-politics 'free for all'—in Rovner and Moore, "Does the Internet Need a Hegemon?"; Chris Demchak and Peter Dombrowski, "Cyber Westphalia : Asserting State Prerogatives in Cyberspace," *Georgetown Journal of International Affairs*, 2013, 29–38.
[86] EEAS, "Food-for-Thought Paper 'Countering Hybrid Threats'" 2015, no. May (2015): 8, http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15. pdf.; See also: Johannes Hahn, in Nitoiu and Sus, "Introduction: The Rise of Geopolitics in the EU's Approach in Its Eastern Neighbourhood."
[87] European External Action Service, *Food-for-Thought Paper: 'Countering Hybrid Threats.'*
[88] Patryk Pawlak, "Understanding Hybrid Threats," 2015, https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.

policymakers further realized that cyberspace could be used to exploit actors' dependence on foreign technologies for their own geopolitical aims.[89]

As the Ukraine crisis unfolded, a historically unprecedented number of irregular migrants entered the EU in 2015. This so-called 'migration crisis' exacerbated an already existing trend of *externalisation,* which centred upon the construction of migrants as grave threats to EU citizens' security.[90] As a consequence of the crisis, several EU Member States suspended the Dublin Regulation, which had legislated the distribution of asylum requests amongst all EU countries, and proceeded to engage in a contentious process of 'internal bordering' along national boundaries. This divisive behaviour sparked intense criticisms that the EU had 'lost control over its borders', which converged with growing public opinion that the EU had insufficient external border controls.[91] While the EU had already started to implement digital migration databases to enforce its borders,[92] the crisis reinforced the EU's embrace of the 'security-development' nexus as a principle of its external engagement and the need for promoting EU values and practices overseas.[93] As I explain later in this section, this approach was extended to the EU's approach to external cyber capacity building as a form of development cooperation. From 2015-2018, cybersecurity capacity building emerged as a new priority for external engagement, especially with the EU's Neighbourhood region.[94]

Over this period, the EU's approach to global cyberspace became more external-facing and cross-dimensional, particularly in the areas of defence and security. In 2014, the EU Council designed the Cyber Defence Policy Framework to contend with the growing 'cyber dimension' in many hybrid threats and campaigns.[95] The *European Agenda for Security* (2015), expressed, for instance, that 'EU internal security and global security are mutually dependent and interlinked.'[96] Subsequently, the EU's 2016 *Joint Framework on Countering Hybrid Threats* recognized the potential for cyberspace to be leveraged by 'perpetrators of hybrid threats'—including state actors.[97] This document followed the release of a new *Global Strategy for the European Union* (EUGS) in 2016, which outlined the aspiration for the EU to become a 'forward-looking cyber player.'[98] Consequently, EU cybersecurity policy was reconfigured to become compatible with the EUGS' 'joined-up' strategy, which brought about the further integration of EU cybersecurity policy with the EU's global approach. Particularly, the EUGS aimed to foster 'a Union that builds on the success of 70 years of peace,'—for which 'our

---

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

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

[91] Philipp Lutz and Felix Karstens, "External Borders and Internal Freedoms: How the Refugee Crisis Shaped the Bordering Preferences of European Citizens," *Journal of European Public Policy 28* no.3 (2021): 370-388, https://doi.org/10.1080/13501763.2021.1882541.

[92] Dennis Broeders, "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants," *International Sociology*, *22* no.1 (2007): 71-92. https://doi.org/10.1177/0268580907070126.

[93] Stephan Keukeleire, and Kolja Raube, "The security–development nexus and securitization in the EU's policies towards developing countries," *Cambridge Review of International Affairs*, *26* no. 3 (2013): 556–572. https://doi.org/10.1080/09557571.2013.822851.

[94] Carver, 2024, 'More bark than bite?'.

[95] Politico-Military Group, *Six Monthly Report on the Implementation of the Cyber Defence Policy Framework,* vol. 2016, 2016.

[96] European Commisssion, *The European Agenda on Security*, Brussels, 2015, 4, https://doi.org/10.4324/9780429465918-2.

[97] European Commission and HRVP, *Joint Framework on Countering Hybrid Threats: A European Union Response*, 10.

[98] European Union, "Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy," 42.

security at home depends upon peace beyond our borders.'[99] Subsequently, the EUGS became a point of reference for the EU's external, spatialized orientation towards global cyberspace.[100]

Demonstrating a stark change to the EU's 2013-era approach to cyberspace, EU officials during this period cited the 'borderless' nature of threats or malicious activities in cyberspace as justifying further *external* intervention, including 'enhancing cyber capacity building action under external assistance instruments.'[101] Outside of the EU's revised conceptual framework of security, this could be seen as peculiar, as if cyber problems are indeed 'borderless', they would not logically merit *external* instruments (which by definition have a bordered aspect), but rather the proportionate use of *all* instruments. However, using 'borderless threats' to justify further external intervention coheres with a key component of the EU's broader security logic, which holds that internal security depends upon external security—or, according to former Commission President Barroso, as requiring more EU investment into external relations.[102] This rationale further echoes the notion of 'my neighbour's and my partner's weaknesses are my own weaknesses' articulated in the EUGS.[103]

For example, the borderless nature of cyberspace was cited as a crucial reason for further extending the EU's external assistance to other countries, as it was seen as a way of reducing cyber insecurities centred around the unpredictability of the EU's neighbours and their (lack of) adherence to established rules of conduct in cyberspace, particularly in light of Russia's 2014 invasion of Ukraine.[104] From 2015-2018, EU-led or funded cyber capacity building programmes were prioritized in the EU's Eastern and Southern Neighbourhoods (e.g. the CyberEast and GLACY++ projects).[105] Arguably, the EU's geographical approach of capacity building programmes during this period reproduced the EU's logic of 'concentric circles' previously deployed to stabilize its (physical) Neighbourhood. As Browning argues, this approach encompasses the process of transforming the EU's periphery in a concentric fashion through incentivizing proximate countries to uptake EU norms and democratic

---

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

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

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

[102] Jose Manuel Durao Barroso, *European Commission 2004 – 2014: A Testimony by the President with Selected Documents*, 22, 2014. This rationale was also voiced by the European Commission, *ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries*, Brussels, 2018, 4.

[103] European Union, *Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign And Security Policy,* European Union, Brussels, 2016.

[104] This rationale was voiced by the European Commission, *ANNEX of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 Part III Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries*, Brussels, 2018, 8. Additionally, interviewed EU officials lamented the lack of clear rules and expectations for safe conduct in cyberspace, which made it difficult to develop a stable understanding of others' behaviour, including in reference to the Ukraine crisis. Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; in Carver, 2024, 'More bark than bite?'.

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

mechanisms with 'conditionality' instruments.[106] Accordingly, CCB programmes have incorporated a particular *spatial* understanding of the cyber environment in terms of 'European cyberspace' and 'non-European cyberspace.'

Externalising border practices are further exemplified by the EU's *General Data Protection Regulation* (GDPR), which instantiates the export of EU rules and best practices to the external environment to improve (economic and cyber) security at home. Produced in 2016, the GDPR marks a significant change in policy instruments from its 1995 legal predecessor,[107] especially in terms of the territorial scope of its application, which has expanded to include data controllers/processors not established in the EU. The GDPR's Article 45 stipulates that data may be transferred from within EU borders to third countries providing there is an 'adequate level' of data protection guaranteed by the country, in accordance with EU legal standards.[108] As Joanne Scott argues, the GDPR constitutes a form of *territorial extension* which 'depends upon the existence of a relevant territorial connection, but where the relevant regulatory determination will be shaped as a matter of law, by conduct or circumstances abroad.'[109] Specifically, the territorial reach of the GDPR is centred around two criteria: 1) data controllers established in the EU and 2) the 'targeting' of EU citizens.[110] Therefore, the influence and success of GDPR is reliant upon (and reproduces) the EU's territoriality and European citizenship in the digital domain.

The importance of the GDPR for the EU's projection of power over the global digital domain should not be understated—it has been heralded as one of the EU's 'greatest achievements', 'the gold standard all over the world.'[111] The GDPR has already shaped the development of many third countries' data protection legislation (viz. the UK, the US, and some African countries, including Nigeria and Kenya).[112] Accordingly, scholars have described the EU's promotion of the GDPR in the context of development cooperation as a 'soft form' of

---

[106]For further reference, see Christopher Browning, "Geostrategies, Geopolitics and Ontological Security in the Eastern Neighbourhood: The European Union and the 'New Cold War,'" *Political Geography* 62 (2018): 106–15, https://doi.org/10.1016/j.polgeo.2017.10.009; and Luiza Bialasiewicz, *Europe in the World: EU Geopolitics and the Making of European Space* (Routledge, 2015).

[107] European Parliament and Council of the European Union, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," No. 31995L0046 (1995).

[108] European Parliament and Council of the European Union, "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Da" (2016).

[109] Joanne Scott, "Extraterritoriality and Territorial Extension in EU Law," *The American Journal of Comparative Law* 62, no. 1 (2014): 90; see also Christopher Kuner, "The Internet and the Global Reach of EU Law," in *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, ed. Marise Cremona and Joanne Scott (Oxford University Press, 2019).

[110] European Data Protection Board*, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation*, (2018): p. 3. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf

[111] European Data Protection Supervisor, "The History of the General Data Protection Regulation ," 2022, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[112] Interviewee E, interview by author, virtual (online video), March 25, 2021, in Carver, 2024, 'More bark than bite?'; see also: Annegret Bendiek and Magnus Römer, "Externalizing Europe: The Global Effects of European Data Protection," *Digital Policy, Regulation and Governance* 21, no. 1 (2019): 32–43, https://doi.org/10.1108/DPRG-07-2018-0038; John Campbell, "Nigeria's Slide Toward Authoritarianism," Council on Foreign Relations, January 15, 2020, https://www.cfr.org/in-brief/nigerias-slide-toward-authoritarianism., Brian Daigle, "Data Protection Laws in Africa : A Pan- African Survey and Noted Trends," *Journal of International Commerce and Economics*, no. February (2021): 1–27, https://www.usitc.gov/staff_publications/all; Sharon Tan and Nurul Syahirah Azman, "The EU GDPR's Impact on ASEAN Data Protection Law ," Financier Worldwide, accessed March 25, 2022, https://www.financierworldwide.com/the-eu-gdprs-impact-on-asean-data-protection-law.

geopolitics, wherein the EU pursues the development of certain geographical space in tandem with the promotion of EU values and norms.[113]

One year later following the publication of the GDPR, the 2017 strategy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,* emphasized the EU's goals to encourage 'due diligence and state responsibility in cyberspace', and for the EU to achieve 'greater resilience and strategic autonomy.'[114]The strategy, drawing upon the experiences of Ukraine and other destabilizing events during this period, emphasized that 'the continuously evolving and deepening threat landscape calls for more action to withstand and deter attacks in the future.'[115] Notably, the 2017 update followed the release of the *Reflection Paper on the Future of European Defence* (in which cybersecurity was a key priority), which stressed that further cooperation at the EU level and an enhanced role for the EU would strengthen Member States and make them 'more sovereign.'[116] This striking statement, which established a clear link between collective European approach to security and the national sovereignties of Member States, would foreshadow the widespread uptake of '*European* digital sovereignty' in future EU strategic documents.

The 2020 cyber strategy: *Reterritorialization* and the rise of geopolitical and sovereigntist claims in EU discourse

The Union's engagement with bordering practices throughout the development of the 2013 and 2017 strategies were the precursor to a more consolidated '*EUropean*' recognition of cyberspace as a geopolitical environment. After the release of the 2017 European cyber strategy, debates about the cybersecurity risks of Huawei 5G infrastructure were another 'wake-up call' for EU policymakers, cementing their fears about digital dependency.[117] Whereas official EU discourse about foreign dependency had previously revolved around private companies alone—including in 2013 cyber strategy[118]--the Huawei debate popularized fears that Europe could become subject to the *(geo)political* motives of foreign *state* actors through the dependency on foreign technologies. In other words, it demonstrated to EU officials the 'increasing entanglement' of power politics between states and *digital geopolitics*.[119] As Chinese companies comprise a large portion of shares in the European telecommunications market and enjoy better (Chinese state-funded) subsidies compared to their European counterparts, concerns have been raised about foreign direct investment in 5G and other digital

---

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

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

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

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

[117] Interviewee B, interview by author, virtual (online video), March 11, 2021; in Carver, 2024, 'More bark than bite?'.

[118] European Union Committee, *Protecting Europe against Large-Scale Cyber-Attacks* 2010; Council of the European Union, *Proposal for a Directive 2013/27(COD) Concerning Measures to Ensure a High Common Level of Network and Information Security across the Union*. Brussels, 2013, 4, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf..

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

technologies.[120] This was later reiterated in a broader sense within the Commission's progress report on *The Security Union* in October 2019, which noted the importance of the 'risk profile of individual suppliers', which would be determined in part by the 'likelihood of the supplier being subject to interference from a non-EU country.'[121] This debate motivated the development of the EU's '5G Toolbox' regulation, which was impelled by the urgency to achieve Europe's digital sovereignty before the Union 'falls behind.' [122]

Accordingly, the Union's explicit approach to geopolitics and its self-representation as a geopolitical actor changed significantly under the leadership of Ursula von der Leyen (the EU's Commission President) and Josep Borrell (HR/VP of the EEAS). Josep Borrell asserted that the EU's 2020 cyber strategy reflects the imperative for 'the EU [to] learn the language of power and act geopolitically'[123]—laying bare that cyberspace is understood is not a challenge, but an *enabler* for the EU's geopolitical agenda. Over this period, the COVID-19 pandemic 'forcefully revive[d] the central question of [Europe's] autonomy, our sovereignty and our position as a player in world geopolitics, particularly in the face of growing tensions between the United States and China.'[124]

Currently, Brussels envisions 'a world of rivalries, especially between the US and China…with technology as a major fault line and cyber as the new domain.'[125] Evidently, constructing cyberspace within a traditional geopolitical framework—even if it is a poor conceptual fit—draws upon familiar notions of (state-based) strategic competition. [126] Such a conception, in turn, can be seen to beg a geopolitical response. Accordingly, over the past five years, Brussels, in explicit competition with the US and China,[127] has increasingly turned towards investing in shaping the structural features of cyberspace. In 2021, Brussels devoted €300 billion to its *Global Gateway* connectivity project as an alternative to China's Belt and Road Initiative and American infrastructure funding, aimed at promoting the 'European model of trusted connectivity' in the areas of digital (with integrated cybersecurity aspects), climate and energy, transport, health, education and research.[128]

However, for the EU as a global actor, invoking geopolitical frames comes into tension with its 'origin myth' as eschewing geopolitics.[129] Indeed, the EU's agnosticism towards

---

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

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

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

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

[124]Op-ed published by the European Union External Action Service, "For a united, resilient and sovereign Europe (with Thierry Breton)," June 6, 2020, https://www.eeas.europa.eu/eeas/united-resilient-and-sovereign-europe-thierry-breton_und_en.

[125] Borrell, 2020.

[126] Eberle and Daniel, 2022.

[127] "THIS ACTION IS FUNDED BY THE EUROPEAN UNION ANNEX 3 of the Commission Implementing Decision on the financing of the annual action plan in favour of the United Republic of Tanzania for 2021" Link: https://www.gtai.de/resource/blob/788132/e262205f40141c2ea2c13c84f61c4b27/PRO20220127788124%20-%20Annex3.PDF.

[128] European Commission, 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.

[129] Nora Fisher Onar and Kalypso Nicolaïdis, "The Decentring Agenda: Europe as a Post-Colonial Power," *Cooperation and Conflict* 48, no. 2 (2013): 283–303, https://doi.org/10.1177/001083671348538; Stefano Guzzini, *The Return of*

geopolitics in the context of its own policymaking has been a longstanding discursive trend,[130] and it is closely tied together with the EU's 'founding myth' for its political existence. Whereas the EU had once drawn clear distinctions between its 'Self' and geopolitical 'Others', it would appear that this demarcation would no longer hold. Thus, it is conceivable that the transition to openly taking a 'geopolitical perspective' would elicit anxieties reconciling the EU's historical self-representation with its contemporary outlook and future ambitions.

My interviewee responses indicate such insecurities, suggesting that, while geopolitical conversations had become normalized and even encouraged by the late 2017-2020 period by the EU's allies (with the President Biden's election), the capacity to 'speak in geopolitical terms' has been constrained by enduring cultural expectations (and anxieties) about the EU's self-representation as a non-geopolitical actor.[131] To explain the EU's intentions in cyberspace, interviewees frequently contrasted the EU with 'traditional' (Westphalian) geopolitical actors: China, Russia, and the United States. In distinction to these foreign policy players, EU interviewees described the EU as post-Westphalian insofar as it lacked the trappings—and competences—of nation states in the area of security.[132] 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.[133] Clearly, 'geopolitics' still constituted an important demarcation between the EU's role in the world and those of other actors for interviewees: despite the EU's transition to speaking 'in geopolitical terms', EU officials have continued to distance the EU from geopolitical actors when representing the EU's role in the world.

This tension raises the question: since the EU was not originally designed to be a geopolitical actor in terms of capabilities or aspiration, how can we make sense of the EU's geopolitical role today? The discourse of 'European digital sovereignty', I have argued elsewhere,[134] seeks to recast the EU's new role as an avowedly geopolitical actor by appealing to an historically legitimate politico-legal concept: sovereignty. At the same time, it establishes a distinction (albeit a vague one) between a *European* form of sovereignty—including vis-a-vis Member State *sovereignties*—and those advanced by outside actors. This argument is briefly illustrated below.

European digital sovereignty discourse as differentiation

European digital sovereignty discourse can be understood as a bordering practice for the EU: to differentiate the European approach from external actors *and* to bring together its internal constituents. In his 2018 *State of the Union* speech, former EU Commission President Juncker laid out the distinctively 'European' conception of sovereignty: that it was 'shared internally' and 'unified externally.'[135] Juncker argued that rather than militarization and protectionism, 'the Euro must become the face and the instrument of a new, more sovereign

---

Geopolitics in Europe?: Social Mechanisms and Foreign Policy Identity Crises (Cambridge: Cambridge University Press, 2012), 6, https://doi.org/doi:10.1017/CBO9781139225809.

[130] See also: David Cadier, "The Geopoliticisation of the EU's Eastern Partnership," *Geopolitics* 24, no. 1 (2019): 71–99, https://doi.org/10.1080/14650045.2018.1477754; Thomas Diez, "Europe's Others and the Return of Geopolitics," *Cambridge Review of International Affairs* 17, no. 2 (2004): 319–35, https://doi.org/10.1080/0955757042000245924.

[131] Carver, 2024, 'More bark than bite?'

[132] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee F, interview by author, virtual (online video), April 15, 2021; in Carver, 2024, 'More bark than bite?'.

[133] Interviewee C, interview by author, virtual (online video), March 12, 2021; in Carver, 2024, 'More bark than bite?'.

[134] Carver, 2024, 'More bark than bite?'.

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

Europe.'[136] In turn, European digital sovereignty discourse was a key pillar for the current von der Leyen's electoral platform in 2019. 'European digital sovereignty,' as I have argued elsewhere, has been increasingly framed by EU documents 'as the solution to multiple concerns: the cybersecurity risks of using Chinese technology for critical European infrastructure, the increasingly outsized role of foreign tech giants in shaping the European digital ecosystem, including data and AI, the socio-economic and geopolitical risks of competitive US-China dynamics, and the lack of a 'level playing field' for European technology firms in foreign markets and in global digital value chains.'[137]

By emphasizing the EU's particular values and economic capabilities, Brussels has sought to differentiate itself from the invasive and *Westphalian* geopolitical aims of other global cyber actors (particularly Russia and China) and from the competitive goals of the US.[138] Particularly, leveraging the economic assets of the EU for the current 'geopolitical hour'[139] emphasizes the EU's material (economic) capabilities—rather than classical military might—differentiates the EU from other classical geopolitical actors. 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.'[140]

Adopting the language of 'sovereignty' to explain the EU (and Europe's) increased role in cyberspace constructs Europe as taking up its *rightful* place in cyberspace and asserting its *sovereign, legitimate* authority to ensure the future of European existence in global cyberspace. The distinctiveness—and autonomy—of Europe in cyberspace has been expressed in a multitude of policy documents, including the Commission's 2020 Communication, *Shaping Europe's Digital Future,* which has defined European technological sovereignty 'by focusing on the needs of Europeans and of the European social model.'[141] As the Commission reasoned, the concept of European digital sovereignty is necessary as Europe 'needs to be a strong, independent and purposeful digital player *in its own right*.'[142]

Relatedly, scholars have suggested that the European digital sovereignty concept may aim to establish broader cohesion within the EU security community. In this vein, Csernatoni has asserted that digital sovereignty discourse has helped to 're-cent[er]' these policy spaces 'as sites of legitimate hegemonic intervention for EU-level competence and governance.'[143] Nevertheless, Juncker's aspiration for a 'shared internal' conception of European digital

---

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

[137] Carver, 2024, 'More bark than bite?', p. 2265. See also European Commission, "EU-US launch Trade and Technology Council to lead values- based global digital transformation," June 15, 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2990; European Commission & High Representative of the Union for Foreign Affairs and Security Policy, *EU-China—A Strategic Outlook* [JOIN(2019) 5 final].

[138] 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. For reference, see Carver, 'Developing digital peripheries', 2024; and Patryk Pawlak and Nayia Barmpaliou, *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building: Second Edition,* 2023 (Tallinn: European Union). https://www.eucybernet.eu/wp-content/uploads/2023/11/operational-guidance-for-the-eu-international-cooperation-on-ccb-1-1.pdf.

[139] Juncker, 2018.

[140] Emphasis added, European Council, 2021, "Digital sovereignty is central to 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/.

[141] European Commission*, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's Digital Future, p. 2.*

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

[143] Csernatoni, 2022, p. 397.

sovereignty has not been fully realised. There remains internal contestation between EU policymakers and stakeholders surrounding the usage and meaning of sovereignty in EU policy discourse and thus deep instabilities underlying the concept.[144] Moreover, internal EU contestation regarding the usage of 'autonomy' versus 'sovereignty' has resulted in insecurities about conceptual misunderstandings with other external actors. This is particularly noticeable in interviewee responses, who raised concerns about the EU's misperception as 'an island' by strategic partners and as shirking its strategic transatlantic ties.[145] Despite these conceptual tensions, a key motivator for Member States' support of the 'sovereignty' concept was the realization that Member States could not 'act alone' in the current geopolitical context; for EU policymakers, the concept was seen as necessary to have 'conversations with the big geopolitical powers', including in 5G discussions.[146]

Territorial ordering and the EU bordering practices during the von der Leyen Commission

Furthermore, recent EU policy efforts to regulate foreign direct investment and political influence from non-EU actors, as evidenced with the 5G Toolbox, evince aspects of 'control' and 'closure'. This is further revealed with the Union's struggles to develop a federated European-owned, European-wide cloud infrastructure,[147] to control various private sector initiatives in Europe and globally,[148] and to develop an authoritative Europe-wide cybersecurity community.[149] Additionally, major investments in building the cybersecurity and digital capacities of third countries beyond the EU's Neighbourhood (e.g. the *Global Gateway Initiative*) in recent years illustrate a more ambitious approach to shaping the global digital domain and promoting EU standards, digital infrastructure, and technologies overseas. This may have implications for the territorial ordering of global cyberspace in terms of who has primary control and access over key global networks which form the backbone of internet connectivity.[150] At the very least, these policy developments, most of which have occurred under the banner of 'European digital sovereignty, signal efforts by the EU to compete in and through cyberspace by drawing upon geographic points of control.

Altogether, the confluence of both sovereigntist and geopolitical claims at the supranational level, paired with recent policy developments—including in the areas of cloud computing, foreign direct investment in digital technologies (e.g. 5G), and cybersecurity infrastructure—evince a particular geopolitical imaginary of the EU's role in and through global cyberspace, one compatible with the Single Market and the EU's self-representation as a global technological leader and standard-setter. Externally, European digital sovereignty discourse has established further relational distinctions between the European approach and its partners and rivals; internally, it seeks to foster internal cohesion around a 'EUropean'—not solely state-centric—internal digital environment.

---

[144] Carver, 2024, 'More bark than bite?'.

[145] Interviewee A, interview by author, virtual (online video), March 5, 2021; Interviewee B, interview by author, virtual (online video), March 11, 2021; Interviewee D, interview by author, virtual (online video), March 18, 2021; in Carver, 2024, 'More bark than bite?'.

[146] See also Carver, 2024, 'More bark than bite?', p 2275.

[147] Andreas Baur, "European Dreams of the Cloud: Imagining Innovation and Political Control," *Geopolitics*, 29 no. 3 (2023): 796–820, https://doi.org/10.1080/14650045.2022.2151902.

[148] Farrand and Carrapico, 2021.

[149] For a broader account of struggles for epistemic authority and the development of a European cyberspace, see Myriam Dunn Cavelty and Max Smeets, "Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority," *Journal of European Public Policy*, 30 no. 7 (2023): 1330–1352. https://doi.org/10.1080/13501763.2023.2173274.

[150] For further reference, see Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (OUP, 2023) and Daniel W. Drezner, Farrell, Henry, and Newman, Abraham L., eds., *The Uses and Abuses of Weaponized Interdependence* (Brookings Institution, 2021), https://www.brookings.edu/books/the-uses-and-abuses-of-weaponized-interdependence/.

Summary: Characterizing EU bordering practices in cyberspace over time

This paper identified three defining logics underlying the EU's bordering practices vis-à-vis cyberspace since the inception of its first cybersecurity strategy: *demarcation, externalisation*, and *reterritorialization*. While these logics are not mutually exclusive (demarcation, for example, could be conceived as a form of reterritorialization), they have been characterized by distinctive ideas, events, and political objectives. Throughout all these periods, EU bordering practices are observable and entangled with the EU's evolution as a cyber actor, culminating in the EU's striking turn to sovereigntist and geopolitical logic.

Specifically, in the early 2010s, demarcating between 'European' and 'non-European' cyberspace(s) was critical for enabling the EU to advance a collective European approach to cyberspace. This demarcation laid the basis for 'externalising' threats and insecurities to outside of EU borders as a way of managing the EU's 'existential crisis,' including towards cyberspace and the digital domain more broadly. Such externalisation, particularly in light of the EU's *Global Strategy,* laid the basis for a more assertive EU approach to the world whilst maintaining the conviction that the EU's internal security depended upon securing its external borders.[151]

Contemporaneously, this approach has been built upon and modified by the European digital sovereignty concept. As I argued in this paper, the internal dimension of European digital sovereignty is about asserting (legitimate) control over a bounded space and facilitating closure from dependence on foreign actors. The concept's external dimension comprises a claim to global legitimacy within a particular (global) field of action. Furthermore, European digital sovereignty has served as a *relational* border between 'traditional' geopolitical actors such as China and the US and the EU's own geopolitical approach. The next section reflects upon the implications of EU bordering practices for the EU's evolving role in an increasingly uncertain global environment.

It should be noted that EU bordering practices are not confined to a few policy domains in the EU, but they are integral to the European integration project. Further research could examine how, if at all, EU bordering practices differ across different geographic milieus. One related area for further consideration is how the EU's approaches to bordering have come into tension, or reinforced, national digital territorialization projects within the EU. Scholars have recently explored how states seek to convert digital infrastructure into state power through 'territorializing moves', including sovereigntist claims.[152] This literature serves as a valuable point of departure for making sense of how EU bordering is interpreted, negotiated, and practiced by Member States and European publics.

Reflections on Europe in the (Digital) World: The EU's role in a world of global digital interdependence

In his (2007) book on *Europe as Empire,* Jan Zielonka argued that the enlarging EU would resemble a 'multilevel governance system of concentric circles, fuzzy borders, and soft forms of external power projection resemble the system we knew in the Middle Ages, before the rise of nation states, democracy, and capitalism.'[153] This observation is, in my view, partly correct for the contemporary context. The EU's global approach to the digital domain evinces

---

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

[152] See for instance 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.

[153] Zielonka, "Introduction: The Neo-medieval Paradigm."

varying degrees of 'soft' external power projection (as evidenced by the GDPR and past cyber capacity building initiatives) but also a return to 'geopolitics' and the desire to assert further structural control over global digital infrastructures, as illustrated by the EU's *Global Gateway Initiative*. Accordingly, the EU is not exactly 'becoming a polycentric polity *penetrating rather than controlling its environment*,' as Zielonka predicted.[154] Rather, the EU's bordering practices in and through cyberspace highlight increasing efforts by Brussels to assert functional and territorial control over its internal environment and to actively shape the global domain through a combination of 'hard' and soft policy instruments—from a sanctions toolbox, to infrastructural investments, to cyber diplomacy.[155] The EU's desire to reclaim 'European sovereignty' and ensure 'European strategic autonomy' is responding to a perceived loss of control over its internal environment, particularly in the digital domain *and* to anxieties about dependence on foreign actors for critical services and technologies—that is, fears about foreign penetration into core European services and goods. At the global level, we may be experiencing the rise of 'digital empires'—the EU included (to use Anu Bradford's terminology)[156]—but they are reliant upon both penetration *and* control.[157]

Historicizing the EU's contemporary turn to European digital sovereignty and geopolitics with attention to *bordering practices* produces several insights about the EU's role as a global actor. First, historical continuities *and* changes have defined the EU's engagement with territoriality in and through cyberspace. Previously, the EU has tended to focus its attention on its 'borderlands' through various cyber capacity building projects—including the CyberEast programmes in its Eastern Neighbourhood, and the GLACY++ initiatives in the Southern Neighbourhood, although it has become more ambitious in recent years.[158] By and large, then, the EU's cyber capacity building initiatives can be understood to reproduce familiar approaches to threat externalisation and stabilizing its external environment through exporting EU rules and practices, as situated within the EU's wider approach to development cooperation.[159] Continuity is also evident in how the EU has justified its leadership aspirations in the digital domain, which have been primarily advanced on the basis of its historically prominent role as a technological leader and standard setter.[160] For example, to promote the EU's 2020 *Digital Strategy,* the Council of the EU concluded 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.*'[161]

However, the changing context of the digital domain has also spurred further changes in the EU's self-positioning, with potentially significant implications for the coherence of the EU's identity as a global actor. Externally, while the EU has officially stated that European

---

[154] Ibid.
[155] Carver, 'More bark than bite?', 2024.
[156] Bradford, 2023.
[157] See Vili Lehdonvirta, *Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control* (MIT Press: 2024); Lars Gjesvik, ""Private Infrastructure in Weaponized Interdependence." *Review of International Political Economy* 30 no. 2 (2021): 722-746. Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44 no. 1 (2019): 42–79.
[158] See for instance the EU's 2021 Global Gateway strategy.
[159] Carver, 'More bark than bite?', 2024. However, they have also evolved in important ways regarding their strategic importance. See for instance Robert Collett and Nayia Barmpaliou, "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; Patryk Pawlak, "Capacity Building in Cyberspace as an Instrument of Foreign Policy," *Global Policy* 7 no. 1(2016): 83-92.
[160] Eberle and Daniel, 2022; Anu Bradford, The *Brussels Effect: How the European Union Rules the World* (Columbia Law School, 2020).
[161] Emphasis added. General Secretariat of the Council, *Shaping Europe's Digital Future - Council Conclusions*, 13.

digital sovereignty is *not* defined against others,[162] I have averred that '*European* digital sovereignty' has been leveraged to differentiate the EU from other actors in this geopolitical context. In this regard, 'European digital sovereignty discourse' has served to reinforce the position of the EU as a geopolitical actor vis-à-vis the US and China.[163] At the same time, EU policymakers have framed the Union as *transcendent* of classical state-based geopolitics.

Yet, I have shown that the EU has consistently engaged with bordering practices to delineate the boundaries of 'digital Europe' from the first EU cyber strategy in 2013. As Merje Kuus points out, 'even claims about "escaping" geography and geopolitics are geopolitical insofar as they assume a particular geographical configuration of power that is to be eluded.'[164] The (re)territorialization of cyberspace, then, must be understood within the broader project of placing Europe and/or EUrope on the contemporary geopolitical map.

By drawing upon the *European social model* and the lessons of Europe's historical role as a technological leader (as referenced above),[165] European digital sovereignty discourse has been invoked to manage these tensions. I have suggested that this discursive manoeuvring has been partly driven by internal anxieties; as an effort to overcome the EU's historical baggage with 'geopolitics' as a pillar of its political identity. However, the discourse has not resolved these tensions; rather it may have created further challenges for the EU's future coherence as a global actor. As Broeders, Cristiano, and Kaminska put it, European digital sovereignty discourse has 'inherent tensions with the EU's normative power in digital issues and may also result in strategic cacophony.'[166]

Particularly, such discourse may have implications for the EU's approach to individual digital freedom, which remains an unresolved tension with the digital sovereignty concept. As Barrinha and Christou observed, 'The potential paradox between imposing one's will and ensuring the system remains open is not acknowledged [by the EU] as a potential problem.'[167] This is clearly illustrated in the 2022 *Council Conclusions* on *Digital Diplomacy*, which outlined the following objectives: The EU's current objective is to 'Promote an open, free, global, stable and secure Internet based on the multi-stakeholder model of Internet governance' (p. 3). At the same time, the *Conclusions* stated that the Union is seeking to 'Improve 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,' (ibid, p. 5). Overall, it appears that neither 'geopolitics' nor 'sovereignty' concepts have been panaceas for the EU's longstanding identity crisis, nor its efforts to manage a rapidly evolving world.

In conclusion, exploring EU bordering practices in and through cyberspace demonstrates that the changing digital environment has provided opportunities for the EU to expand its role in external relations and to reconstitute the boundaries of 'Europe' in a globally connected world. The EU's changing security environment and its increasing entanglement

---

[162] European Commission*, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's Digital Future, p. 2.*

[163] Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty - Rhetoric and reality. Journal of European Public Policy, 1–22. https://doi.org/10.1080/13501763.2024.2358984. This is also suggested by my interview data, discussed in the previous section.

[164] Meerje Kuus, *Geopolitics Reframed : Security and Identity in Europe's Eastern Enlargement* (Palgrave Macmillan: 2007)*,* p. 7.

[165] See also Eberle and Daniel, 2022.

[166] Dennis Broeders, Fabio Cristiano, and Monica Kaminska, "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 (2023): 1261–1280. https://doi.org/10.1111/jcms.13462.

[167] André Barrinha and Georges Christou, "Speaking sovereignty: The EU in the cyber domain," *European Security*, 31 no.3 (2022): 370. https://doi.org/10.1080/09662839.2022.2102895 2022.

with digitalization, cybersecurity challenges, and geopolitical competition has elevated the significance of cyberspace for the EU's strategic agenda and spurred significant changes in the Union's foreign policy behaviour towards geopolitical and sovereigntist objectives. However, this behavioural shift has also introduced further tensions and challenges for the EU's development as a global actor. As geopolitical competition continues to escalate in the digital domain, particularly with developments in artificial intelligence and cloud computing, EU (re)bordering practices are likely to be a defining characteristic of the EU's external action beyond the 'Digital Decade.' Moreover, so long as EU bordering practices towards cyberspace remain associated with sovereigntist and geopolitical goals, they have potentially significant implications for the exercise of individual (digital) freedom within the Union and outside its borders.

Acknowledgements

I would like to gratefully acknowledge Nuffield College and the Economic and Research Council for funding my research [ES/P000649/1], and the Dahrendorf Programme for their support. This essay draws from two published articles[168] I have written as part of my dissertation research, which have been cited throughout the essay where relevant (see footnote 1).

[168] Julia Carver, "More bark than bite? European Digital Sovereignty Discourse and Changes to the European Union's External Relations Policy," *Journal of European Public Policy* 31 no. 8 (2024): 2250–86, doi:10.1080/13501763.2023.2295523; and Julia Carver, "Developing Digital "peripheries" for Strategic Advantage: Capacity Building Assistance and Strategic Competition in Africa," *Contemporary Security Policy* (2024): 1–42, doi:10.1080/13523260.2024.2430021.