JCMS JOURNAL OF COMMON MARKET STUDIES UACES

JCMS 2024 Volume 00. Annual Review pp. 1–12 DOI: 10.1111/jcms.13654

Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics

HELENA CARRAPICO[1] and BENJAMIN FARRAND[2]

[1]Social Sciences Department, Northumbria University, Newcastle upon Tyne [2]Law School, University of Newcastle, Newcastle upon Tyne

Introduction

The European Union (EU)'s cybersecurity policy has, over the past two decades, undergone dramatic changes that have positioned it not only at the forefront of the EU's security policy landscape but also as one of the most influential policies across the EU policy spectrum (Carrapico and Farrand, 2020; Christou, 2015; Dunn Cavelty, 2013; Obendiek and Seidl, 2023). Over the years, the EU has become particularly aware of its increasing reliance on digital infrastructure and services, namely, how sectors such as transport, trade, finance, health, energy and education rely on accessing secure information and communication technology infrastructure. This dependency has been understood as highlighting the EU's vulnerability to the exponential growth in cyberthreats online (Carrapico and Farrand, 2021). Having developed mainly in a reactive fashion to these perceived vulnerabilities, the EU's cybersecurity strategy was officially introduced in 2013 as an umbrella for a set of pre-existing, albeit scattered, initiatives (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013). Since then, it has transitioned from a set of foundational measures to a mature, comprehensive and strategic policy focused on resilience, co-operation and technological advancement. It is composed of four main sub-policy areas: cybercrime and law enforcement; critical information infrastructure protection; cyber-defence; and cyber-diplomacy. Although distinct in their focus, these areas all work together towards the protection of the EU's digital infrastructure and residents.

The evolution of the EU cybersecurity policy can be characterised as having three distinct phases: the first was the genesis phase (1985–2003), during which the different sub-fields of cybersecurity developed separately (in particular in the context of the former EU First and Third Pillars), and the EU gradually positioned itself as a co-ordinating actor capable of addressing cross-border cybersecurity threats. This phase saw the initial recognition of the need for a co-ordinated approach to cybersecurity within a European framework. The second was the institutionalisation phase (2004–2018), where the EU pushed towards a more consistent policy framework by advocating for coherence and dialogue between the different sub-fields. This push involved the introduction and expansion of the number of EU cybersecurity co-ordinating bodies and adopting resilience as a strategy to protect businesses, public bodies and citizens. The third phase can be classified as the regulatory phase (2019–present), which has been marked by a significant attempt by the EU to gain control of cybersecurity governance. This has been achieved through a discursive framing of cybersecurity as a matter of European sovereignty (Farrand and

Carrapico, 2022), the translation of this discourse into a substantial body of legislation (Farrand and Carrapico, 2022; Heidebrecht, 2024), the continued expansion of the number of EU bodies involved in this field and the introduction of international leadership ambitions in this field (Carver, 2023). Overall, the history of EU cybersecurity policy is one of continuous expansion and systematisation, having emerged as *ad hoc* initiatives aimed at protecting the common market and, at a later stage, at furthering the EU Justice and Home Affairs agenda. Having outgrown these policy areas, EU cybersecurity is now also firmly present within the Common Foreign and Security Policy (CFSP) and beyond, making it a truly transversal policy.[1]

The present article analyses the 2023 developments in EU cybersecurity, placing them in their broader geopolitical and policy contexts. In the geopolitical context, the Commission perceives the EU as vulnerable to new threats, and their technological dimension, in a world that is increasingly polarised and unstable. In terms of policy, this has translated into the pursuit of regulatory controls aimed at creating a unified approach to cybersecurity in the Union, characterised by increased oversight and hierarchical EU governance, along with actions aimed at exporting its cybersecurity norms as international standards through cyber-diplomacy initiatives. The article proposes that developments in this field can be understood through the lens of regulatory mercantilism (Farrand and Carrapico, 2022). This framework highlights that there has been a unification of sovereignty, security and economy discourses, in which the EU frames its own vulnerabilities to external threats as necessitating increased regulatory control and exports of its own norms and values as international standards (Farrand, 2023). Regulatory mercantilism is characterised by a rhetorical performativity (Couture and Toupin, 2019) that 'contrasts the geopolitical, security and economic challenges that the EU is facing in the twenty-first century with the vision it has for its future as an integration project' (Bellanova et al., 2022, p. 348). In this sense, regulatory mercantilism identifies policy formation as a means of state-building in response to geopolitical concerns, which this article aims to unpack. It does so by taking the three characteristics of regulatory mercantilism and applying them to the 2023 developments in cybersecurity policy. The first section highlights the EU's growing sense of geopolitical insecurity and vulnerability as a driver of policy; the second explores those policies in more depth, identifying the increased regulatory control the EU is seeking to exert in this policy domain; and the third reflects on the attempts at norm exporting through cyber-diplomacy.

I. Geopolitics and Vulnerability: The New Paradigm of EU Cybersecurity Policy

The EU's 2023 actions in the field of cybersecurity are best understood in relation to the broader policy agenda and initiatives of the EU. With the formation of the von der Leyen Commission, a discourse of 'digital sovereignty' became central to the EU's actions in technology governance (Bellanova et al., 2022). The EU's digital sovereignty discourse expresses a desire for increased control as a response to a perceived sense of vulnerability

[1] Most legislative instruments within this policy field are adopted through Ordinary Legislative Procedure. The legal basis of the instruments reflects the sub-field of cybersecurity policy, with those relating to cybercrime and law enforcement being based on Articles 82 and 83 of the Treaty on the Functioning of the European Union, those on critical information infrastructures and the protection of the common market being based on Articles 114 and 173 and those relating to the Common Foreign and Security Policy before (CFSP) being based on Article 215.

to external threats posed by both non-EU states and private sector actors that may not align themselves with EU values or interests (Carrapico and Farrand, 2020). Shaping Europe's Digital Future, the Commission's policy agenda concerned with the 'digital pillar' of its 2019–2024 work programme framed this sovereignty ambition in terms of developing EU capabilities and reducing external dependencies (European Commission, 2020b, p. 3). It is closely linked to the concept of strategic autonomy (Broeders et al., 2023). The State of the Union 2023 underscores that this European sovereignty is 'an economic and national security imperative to preserve a European edge on critical and emerging technologies' (von der Leyen, 2023, p. 7), reinforcing this notion that EU security is determined by its ability to act independently of external constraints or pressures. These constraints include, namely, a lack of control over externally held or operated infrastructures, services and content providers (Madiega, 2020) with implications for the EU's capacity to protect citizens' data and security (Celeste, 2021; see also Chander and Sun, 2023); a dependence upon critical natural resources possessed or processed by other states required for producing technologies needed for cybersecurity purposes (DeCarlo and Goodman, 2022); and a perceived vulnerability to increased cyberthreats, whether in the form of disinformation, ransomware attacks, denial of service attacks or data breaches (Moerel and Timmers, 2021).

These identified digital vulnerabilities are closely related to the EU's broader sense of its own geopolitical vulnerabilities. This has often been implied in concerns expressed over challenges to the liberal international order as a rejection of globalisation (Braw, 2024), with increased disregard for international organisations and norms (Stephan, 2023) and a return to 'great power' politics between larger states (Weiß, 2023). In the context of these geopolitical changes, there has been a blurring of 'cyber' and 'material' security, with the EU discussing concerns over 'hybrid' threats in 2016 (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016), with cybersecurity being one means by which hostile actors could destabilise the EU, whether through spreading disinformation or attacking critical information infrastructures (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016, p. 10). This 2016 document was followed up in 2018 by a Communication on increasing resilience and bolstering capacities to address hybrid threats, where it was stated that 'cybersecurity is critical to both our prosperity and security. As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed' (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2018, p. 7).

In 2023, the Russian war on Ukraine served to highlight the EU's perceived cyber-vulnerability resulting from broader geopolitical instability, with CERT-EU[2] monitoring the potential for Russia's actions to expand into cyber-operations against the EU's institutions. One of CERT-EU February 2023 report's key findings was that 'cyber operations associated with Russia's war on Ukraine have not been confined to the belligerents. Since Russia's invasion, allies of Ukraine, such as EU countries, have faced several types of cyberattacks' (CERT-EU, 2023, p. 3). New technologies are also classified as

[2] CERT-EU is the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies. It protects the Information and Communication Technology (ICT) infrastructure of all EU institutions and bodies and co-ordinates the response to cyber-incidents.

threats, with generative artificial intelligence (AI) featuring in both the State of the Union 2023 and a report produced by CERT-EU. In the State of the Union, it is explicitly framed as a security threat, with von der Leyen citing experts claiming that preventing human extinction by AI should be prioritised in the same way as preventing nuclear war, stating that AI 'is a general technology that is accessible, powerful and adaptable for a vast range of uses – both civilian and military. And it is moving faster than even its developers anticipated. So we have a narrowing window of opportunity to guide this new technology' (von der Leyen, 2023, p. 9). Similarly, CERT-EU stated that whilst generative AI could have potential cyber-defensive capabilities, they have significant concerns regarding its potential for cyber-offence, with uses including sophisticated social engineering attacks, more effective forms of phishing and automation of the identification of cybersecurity vulnerabilities allowing for the uncovering of previously unknown attack vectors (CERT-EU, 2023, p. 4). Given the concerns regarding the security implications of increased AI use, the European Commission has made clear the desire to regulate the use of the technology internally, through mechanisms such as the AI Act,[3] as well as seeking to guide the development of rules at the international level, both through the AI Act serving as a blueprint for the rest of the world and through guiding innovation and the implementation of minimum standards for safe and ethical use (von der Leyen, 2023, pp. 9–10).

II. All-Encompassing Cybersecurity: Deepening Integration Through Regulatory Control

2023 was a particularly active year for the EU's regulatory efforts in cybersecurity. Whilst admittedly agreed upon at the end of 2022, the directive on measures for a high common level of cybersecurity across the Union (Directive 2022/2555), also known as the NIS2 Directive, entered into force in January 2023. This directive repealed the original NIS Directive and is indicative of a form of regulatory cybersecurity 'state making' on the part of the EU. In its public facing FAQ document, the Commission explained its decision to repeal the original directive and create new legislation on the basis that it was responding to an expanded threat landscape and needed to address 'an insufficient level of cyber resilience of businesses operating in the EU; inconsistent resilience across Member States and sectors; insufficient common understanding of the main threats and challenges across Member States; [and a] lack of joint crisis response' (European Commission, 2023a). The proposal for the directive made clear the desire for increased control in this field, stating that the proposal was part of a package aimed at 'strengthening the Union's strategic autonomy to improve its resilience and collective response' (European Commission, 2020a, p. 1). Interestingly, in the final text of the directive, the link to vulnerability as a basis for intervention is found in recital 37, where it is stated that 'intensified cyberattacks during the COVID-19 pandemic have shown the vulnerability of increasingly interdependent societies' (Directive 2022/2555). As well as updating the pre-existing requirements under NIS1 (Directive 2016/1148), NIS2 provides for stronger oversight and enforcement in order to guarantee resilience from cyberattacks (Vandezande, 2024). Article 12 provides for co-ordinated vulnerability disclosure between member states (MSs), as well as the creation of a vulnerability database that will be maintained by European Union Agency

[3] Whilst an important development, it is not considered explicitly in the context of this article.

for Cybersecurity (ENISA). Article 13 mandates co-operation at the national level between MSs, and Article 14 establishes a co-operation group 'to support and facilitate strategic cooperation and the exchange of information among Member States', the membership of which includes representatives of the MSs, the Commission and ENISA, with the European External Action Service acting as an observer.

2023 also saw a deepening of cybersecurity regulation in line with a regulatory mercantilist frame of heightened oversight and regulatory hierarchy, going from beyond the narrower confines of setting private sector obligations to the establishment of an all-encompassing cybersecurity framework. First, the Commission proposed modifications to the Cybersecurity Act, which had been adopted in 2019 (Regulation 2019/881) to expand its certification schemes to include managed security services. The Commission proposed this as means of raising the overall level of cybersecurity in the Union, which would facilitate the emergence of trusted cybersecurity service providers as a priority for the 'industrial policy of the Union in the cybersecurity field' (European Commission, 2023e, p. 1). The establishment of a European certification system based on European standards was central to the rationale of the Cybersecurity Act (Kohler, 2020), with the expansion of this regime to cover additional sector actors representing a deepening of this regulatory approach. The proposal, which has had its first European Parliament reading and is awaiting the Council's first reading position, states that its purpose is to support the EU Cyber Solidarity Act, which was also published in April 2023 (European Commission, 2023e, p. 2). Interestingly, the main legal basis for the act is Article 173 TFEU, which concerns the creation of the necessary conditions for the competitiveness of the EU's industry, which aligns with the underlying regulatory mercantilist position.

The proposal for the Cyber Solidarity Act makes explicit the link to the digital sovereignty agenda, highlighting the threat posed by external actors with references to Russian aggression and cyberattacks, as well as from other state and non-state actors (European Commission, 2023f, p. 1), strengthening solidarity through better detection of, preparation for, and responses to cybersecurity threats (European Commission, 2023f, p. 2). We see another form of cybersecurity industrial policy being devised within this framework – the means by which these objectives are to be achieved are through the 'deployment of pan-European infrastructure' in the form of security operations centres, named the EU Cyber Shield; the creation of an emergency response mechanism to support MSs in preparing for and responding to cyberattacks, as well as recovering from them; and the establishment of the European cybersecurity incident review mechanism, intended to allow for the review and assessment of significant incidents, with the cybershield and emergency response mechanism being directly funded by the Digital Europe Programme (European Commission, 2023f, p. 3). Article 1 of the proposed Cyber Solidarity Act explicitly includes in its objectives reinforcing 'the competitive position of industry and services in the Union cross the digital economy and contribut[ing] to the Union's technological sovereignty in the area of cybersecurity' (European Commission, 2023f, p. 22), reinforcing the regulatory mercantilist position adopted by the Commission in this field. As of May 2024, the act has secured political agreement between the Parliament and Council and is now awaiting formal approval subject to the Council's first reading (European Commission, 2024).

Two other measures directly focused on cybersecurity also made significant progress in 2023. The EU Cyber Resilience Act, first proposed in September 2022 (European

Commission, 2022), received political agreement in December 2023, was voted favourably by the European Parliament in March 2024 and is now awaiting the Council's first reading (European Parliament, 2024). The purpose of the Cyber Resilience Act, which has Article 114 TFEU as its legal basis, is to ensure that hardware and software products made available in the EU are rendered cybersecure, through measures aimed at guaranteeing cybersecurity through a product's entire life cycle, as well as ensuring that consumers are given sufficient information concerning the security of products, permitting informed choices (European Commission, 2022, p. 2). The act is framed as supporting the Shaping Europe's Digital Future agenda, allowing the EU to 'reap all the benefits of the digital age and to strengthen its industry and innovation capacity, within safe and ethical boundaries' (European Commission, 2022, p. 3). This regulation will give the Commission considerable powers, under the heading of market surveillance and enforcement, including deeming products as non-compliant with the regulation and as presenting a significant cybersecurity risk based on an ENISA assessment. The Commission will then be able to adopt implementing acts applying Union-level restrictions, up to and including withdrawal from the market under Article 45 (European Commission, 2022, p. 59). Interestingly, concerns regarding AI are reflected in the Regulation, with products containing elements classified as high-risk AI systems under the proposed AI Act deemed as falling under the scope of the Cyber Resilience Act under Article 8.

Finally, 2023 saw the formal approval of the EU Institutional Cybersecurity Regulation (Regulation 2023/2841), which was published in the Official Journal in December 2023 and entered into force in January 2024. This regulation obliges all Union entities to have their own internal cybersecurity risk-management, governance and control frameworks under Article 6, the adoption of risk-management measures under Article 8 and to have established a cybersecurity plan by January 2026 under Article 9. Article 10 establishes the Interinstitutional Cybersecurity Board, comprising a representative of each of the Union's entities, which is tasked with monitoring and oversight of compliance with the regulation under Article 11. These combined measures indicate a comprehensive deepening of the EU's cybersecurity regulatory efforts, in which the Commission has fostered a cybersecurity industrial policy, heightening oversight within a regulatory mercantilist framework. As stated by Flonk, Jachtenfuchs and Obendiek, 'even if the EU does not strongly promote the term "digital sovereignty" directly, the volume, bindingness and orientation of its policy output are indicative of a change towards a stronger assertion of its domestic sovereignty' (Flonk et al., 2024, p. 23).

MSs have welcomed these different measures, which they believe to be necessary, at EU level, in order to foster a stronger common level of cybersecurity across the Union. The speed at which the proposals have received political agreement and have progressed through the legislative process, most being adopted following first reading, is indicative of the high level of consensus in this field. MSs have, however, highlighted the need to ensure coherence within this very rapidly expanding policy area and queried the effectiveness of the voluntary nature of some of the proposals (Council of the European Union, 2022b). These are, without doubt, issues that will re-emerge as the field continues to expand.

III. Norm Exporting

As mentioned in the introduction, the third element of the EU's regulatory mercantilist approach to cybersecurity consists in the attempt to export its norms and values beyond its borders with the aim to promote its vision of cybersecurity, and ultimately protect itself from cyberthreats. This ambition is particularly visible in the EU cyber-strategy, which identified international leadership as one of the main priority areas of EU external action (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020). The EU hopes to achieve this leadership through seeking to define and shape international cybersecurity norms and standards, which it is disseminating through its cyber-diplomacy instruments (Latici, 2020). The EU perceives itself as a natural leader in this field and as being uniquely placed to define and promote such standards based on its founding democratic values, respect for the rule of law and fundamental rights. Moreover, it argues that international standards are often being used by non-EU countries to advance 'their political and ideological' visions (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020, p. 20), which are detrimental to EU growth, prosperity and security, making EU action in this field a particularly important priority.

Although EU efforts to become a key cyber-diplomacy global actor are not new (Council of the European Union, 2015; European External Action Service, 2016), we have been able to observe an acceleration in translating this rhetorical ambition into new policy initiatives and diplomatic tools. In practice, this has led to an increased spillover of EU cybersecurity policy from the common market and the area of freedom, security and justice to the CFSP. The new policy initiatives include an increased presence in multilateral bodies, a considerable growth in the number of bilateral agreements the EU has signed and instruments aimed at deepening EU integration (Renard, 2018). Amongst the latter, the 2017 EU cyber-diplomacy toolbox is particularly worthy of mention, as it introduces, for the first time, a joint diplomatic response to malicious cyber-activities (Council of the European Union, 2017). This initiative involves, in particular, a number of CFSP objectives, such as cyber-capability building in third countries, the introduction of EU-led political and thematic dialogues with non-EU countries and the imposing of restrictive measures beyond the EU territory. The Council of the European Union (2022a) has repeatedly stressed the importance of the link between EU external policies, the achievement of its cybersecurity objectives and the ambition to strengthen EU digital sovereignty.

2023 developments in this field further deepened and institutionalised this trend by emphasising the need for 'a stronger, more strategic, coherent and effective EU policy and action in global digital affairs to confirm EU engagement and leadership' (Council of the European Union, 2023, p. 2). More specifically, 2023 saw the EU continue to invest in four main routes to cybersecurity norm exporting: (1) increasing the coherence between cybersecurity policy and other externally facing digital policies, based on the idea that cybersecurity functions as an enabler of advancement in these other policy areas (which include, for instance, the digital promotion of human rights); (2) showing a more united front in international multilateral fora where cybersecurity standards are discussed, such as the International Telecommunication Union and the International Organisation for Standardisation, to ensure greater influence over decisions; (3) increasing the EU's presence in other multilateral organisations where internet governance is being discussed, namely, the United Nations, the World Trade Organisation and the Internet Corporation for Assigned Names and Numbers; and (4) continuing to expand and reinforce the existing network of bilateral and regional partnerships. 2023 saw the launch of the EU-Canada and the EU-Singapore digital partnerships, which prioritise cybersecurity, digital transformation and skills in EU priority areas such as semiconductors, quantum technologies and AI (European Commission, 2023b). Where regional partnerships are concerned, 2023 witnessed the birth of the EU-Latin America and Caribbean Digital Alliance, which focus on capacity building, connectivity, innovation and digitalisation in the region (European Commission, 2023c, 2023d). Finally, this year also saw the proposal to develop structured dialogues directly with the private sector (Council of the European Union, 2023). Although we have observed a considerable effort on the side of the EU to expand its capacity to export cybersecurity norms beyond its borders and to speak with one voice on the international stage, there is for the moment insufficient evidence to ascertain whether this approach is shaping third countries' stance on the topic.

Conclusion

2023 was not a year of grand pronouncements or radical policy shifts in the field of cybersecurity in the EU. Instead, it is a year in which the foundations that have been laid in previous years have been used to further construct a comprehensive EU cybersecurity policy agenda, which can be regarded as being represented by regulatory deepening and active attempts at norm exporting. In line with the explanatory theoretical framework presented in this article, this deepening has been underscored by an explicit securities and vulnerabilities discourse, in which action is required in order to ensure that the EU is able to mitigate against the threats posed to it by external actors and situations over which it feels it has limited control. This perception of limited control has also led the EU to develop a global norm exporting ambition, in line with regulatory mercantilism. As a response to external threats, the EU is seeking to use its regulatory capacity to develop robust standards for cybersecurity internally, which can then be exported to other states and to the international arena in the form of best standards and practices, based on self-described European values, as a means of cementing the EU's position as a global leader, promoting itself as a rule maker rather and in so doing, reducing its vulnerabilities. Through the lens of regulatory mercantilism, we see a blurring of economic and security goals, as well as cybersecurity and material security concerns, centred on the concepts of digital sovereignty and strategic autonomy. In this, EU cybersecurity policy cannot be considered niche or of interest to technical experts only – instead, it serves as a central pillar of the initiatives pursued by the EU in its desire to provide leadership to a world it perceives as presenting myriad complex threats to its continuing stability and security. Finally, given the current evolution of EU cybersecurity, we expect academic research to reflect the exponential expansion of this policy area. In particular, further research is needed to understand how this policy field is being governed, by whom and what impact the digital sovereignty discourse has had (or not) on its advancement. Furthermore, it is important to investigate the implications of the recent surge in EU regulatory cybersecurity measures, not only for the EU as an international leader in cybersecurity but also for its wider search for a more influential position on the world stage. New research in this field will, therefore, need to further examine EU cyber-diplomacy efforts and their implementation, in the context of both multilateral organisations and bilateral relations. From a legal perspective, future research may wish to consider the diverse array of legal bases used for furthering cybersecurity measures, assessing their internal coherence and fit.

Acknowledgements

The authors would like to express their sincere gratitude to the editors of the JCMS Annual Review for their kind invitation to write this piece and for all the comments and suggestions provided.

Correspondence:
Helena Carrapico, Social Sciences Department, Northumbria University, Squires Building, Sandyford Road, Newcastle upon Tyne, UK.
email: helena.farrand-carrapico@northumbria.ac.uk

References

Bellanova, R., Carrapico, H. and Duez, D. (2022) 'Digital/Sovereignty and European Security Integration: An Introduction'. *European Security*, Vol. 31, No. 3, pp. 337–355. https://doi.org/10.1080/09662839.2022.2101887

Braw, E. (2024) *Goodbye Globalization: The Return of a Divided World* (New Haven: Yale University Press).

Broeders, D., Cristiano, F. and Kaminska, M. (2023) 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions'. *Journal of Common Market Studies*, Vol. 61, pp. 1261–1280. https://doi.org/10.1111/jcms.13462

Carrapico, H. and Farrand, B. (2020) 'Discursive Continuity and Change in the Time of Covid-19: The Case of EU Cybersecurity Policy'. *Journal of European Integration*, Vol. 42, No. 8, pp. 1111–1126. https://doi.org/10.1080/07036337.2020.1853122

Carrapico, H. and Farrand, B. (2021) 'When Trust Fades, Facebook Is No Longer a Friend: Shifting Privatisation Dynamics in the Context of Cybersecurity as a Result of Disinformation, Populism and Political Uncertainty'. *JCMS: Journal of Common Market Studies*, Vol. 59, No. 5, pp. 1160–1176.

Carver, J. (2023) 'More Bark Than Bite? European Digital Sovereignty Discourse and Changes to the European Union's External Relations Policy'. *Journal of European Public Policy*, pp. 1–37. https://doi.org/10.1080/13501763.2023.2295523

Celeste, E. (2021) 'Digital Sovereignty in the EU: Challenges and Future Perspectives'. In Fabbrini, F., Celeste, E. and Quinn, J. (eds) *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Oxford, UK: Hart).

CERT-EU. (2023) '*Russia's War on Ukraine: One Year of Cyber Operations – 24 February 2022–24 February 2023*'. CERT-EU. Available from: https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

Chander, A. and Sun, H. (eds) (2023) *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford University Press).

Christou, G. (2015) *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (1st ed. 2016 edition) (Houndmills, Basingstoke Hampshire, New York, NY: AIAA).

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

Council of the European Union. (2017) '*Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities. 13007/17*.' Available from: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

Council of the European Union. (2022a) '*Council Conclusions on EU Digital Diplomacy*. 11406/22.' Available from: https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf

Council of the European Union. (2022b) '*Proposal for a Regulation of the European Parliament and of the Council Laying Down Measures for a High Common Level of Cybersecurity at the Institutions, Bodies, Offices and Agencies of the Union – General Approach*'. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14128_2022_INIT

Council of the European Union. (2023) '*Council Conclusions on EU Digital Diplomacy – Council Conclusions Approved by the Council at Its Meeting on 26 June 2023*. 11088/23.' Available from: https://data.consilium.europa.eu/doc/document/ST-11088-2023-INIT/en/pdf

Couture, S. and Toupin, S. (2019) 'What Does the Notion of "Sovereignty" Mean When Referring to the Digital?' *New Media & Society*, Vol. 21, No. 10, pp. 2305–2322. https://doi.org/10.1177/1461444819865984

DeCarlo, S. and Goodman, S. (2022) 'Russia, Palladium, and Semiconductors'. Executive Briefings on Trade May 2022. US International Trade Commission.

Dunn Cavelty, M. (2013) 'A Resilient Europe for an Open, Safe and Secure Cyberspace'. 23. Swedish Institute of International Affairs.

European Commission. (2020a) 'Proposal for a Directive on Measures for a High Level of Cybersecurity Across the Union, Repealing Directive 2016/1148'. COM(2020) 823.

European Commission. (2020b) 'Shaping Europe's Digital Future'.

European Commission. (2022) 'Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products With Digital Elements and Amending Regulation 2019/1020'. COM (2022) 454.

European Commission. (2023a) '*Directive on Measures for a High Common Level of Cybersecurity Across the Union (NIS2 Directive) – FAQs*'. *European Commission*. 29 June 2023. Available from: https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

European Commission. (2023b) '*EU and Canada Launch Digital Partnership*'. Text. European Commission – European Commission. 2023. Available from: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_5953

European Commission. (2023c) '*EU-LAC Digital Alliance*'. Text. European Commission – European Commission. 2023. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1598

European Commission. (2023d) '*EU-Singapore Digital Partnership|Shaping Europe's Digital Future*'. 2023. Available from: https://digital-strategy.ec.europa.eu/en/library/eu-singapore-digital-partnership

European Commission. (2023e). 'Proposal for a Regulation Amending Regulation 2019/881 as Regards Managed Security Services'. COM(2023).

European Commission. (2023f) 'Proposal for a Regulation Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents'. COM(2023) 209.

European Commission. (2024) '*Political Agreement on Cyber Solidarity Act*'. Text. European Commission. 6 March 2024. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy. (2013) 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace'. JOIN(2013) 1. Brussels.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2016) 'Joint Framework on Countering Hybrid Threats'. JOIN(2016) 18.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy. (2018) 'Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats'. JOIN(2018) 16.

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

European External Action Service. (2016) 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy'. Brussels.

European Parliament. (2024) '*Cyber Resilience Act: MEPs Adopt Plans to Boost Security of Digital Products*'. European Parliament. 12 March 2024. Available from: https://www.europarl.europa.eu/news/en/press-room/20240308IPR18991/cyber-resilience-act-meps-adopt-plans-to-boost-security-of-digital-products

Farrand, B. (2023) 'Regulating Misleading Political Advertising on Online Platforms: An Example of Regulatory Mercantilism in Digital Policy'. *Policy Studies*, pp. 1–20. https://doi.org/10.1080/01442872.2023.2258810

Farrand, B. and Carrapico, H. (2022) 'Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity'. *European Security*, Vol. 31, No. 3, pp. 435–453. https://doi.org/10.1080/09662839.2022.2102896

Flonk, D., Jachtenfuchs, M. and Obendiek, A. (2024) 'Controlling Internet Content in the EU: Towards Digital Sovereignty'. *Journal of European Public Policy*, pp. 1–27. https://doi.org/10.1080/13501763.2024.2309179

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

Kohler, C. (2020) 'The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization'. *International Cybersecurity Law Review*, Vol. 1, No. 1, pp. 7–12. https://doi.org/10.1365/s43439-020-00008-1

Latici, T. (2020) '*Understanding the EU's Approach to Cyber Diplomacy and Cyber Defence*. European Parliamentary Research Service. PE 651.93.' Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf

Madiega, T. (2020) '*Digital Sovereignty for Europe*'. PE 651.992. European Parliamentary Research Service, European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Moerel, L. and Timmers, P. (2021) *Reflections on Digital Sovereignty. SSRN Scholarly Paper ID 3772777* (Rochester, NY: Social Science Research Network) Available from: https://papers.ssrn.com/abstract=3772777

Obendiek, A.S. and Seidl, T. (2023) 'The (False) Promise of Solutionism: Ideational Business Power and the Construction of Epistemic Authority in Digital Security Governance'. *Journal of European Public Policy*, Vol. 30, pp. 1305–1329. https://doi.org/10.1080/13501763.2023.2172060

Renard, T. (2018) 'EU Cyber Partnerships: Assessing the EU Strategic Partnerships With Third Countries in the Cyber Domain'. *European Politics and Society*, Vol. 19, No. 3, pp. 321–337. https://doi.org/10.1080/23745118.2018.1430720

Stephan, P.B. (2023) *The World Crisis and International Law: The Knowledge Economy and the Battle for the Future* (Cambridge, United Kingdom, New York, NY: Cambridge University Press).

Vandezande, N. (2024) 'Cybersecurity in the EU: How the NIS2-Directive Stacks up Against Its Predecessor'. *Computer Law and Security Review*, Vol. 52, No. April, 105890. https://doi.org/10.1016/j.clsr.2023.105890

Leyen, U. von der. (2023) '2023 State of the Union Address by President von der Leyen: Answering the Call of History'. SPEECH/23/4426.

Weiß, W. (2023) 'The EU's Strategic Autonomy in Times of Politicisation of International Trade: The Future of Commission Accountability'. *Global Policy*, Vol. 14, No. S3, pp. 54–64. https://doi.org/10.1111/1758-5899.13147