Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity

Authors:

Benjamin Farrand[1], Newcastle Law School, Newcastle University (United Kingdom) | ben.farrand@newcastle.ac.uk

Helena Carrapico[2], Department of Social Sciences, Northumbria University (United Kingdom) | helena.farrand-carrapico@northumbria.ac.uk

Abstract

In recent years we have been able to observe the emergence and mainstreaming of a EU discourse on digital sovereignty, which highlights the importance of gaining back control of EU digital infrastructure and technological production, based on the EU's perceived loss of economic competitiveness, limited capacity to innovate, high degree of dependence on foreign digital infrastructures and service providers, and, related to all these factors, difficulty in providing EU citizens with a high level of cybersecurity. Bearing in mind that a considerable percentage of these infrastructures and service providers are under private sector control, the present article asks how this sovereignty discourse conceptualises the role of the private sector in EU cybersecurity. Drawing from a Regulatory Capitalism theoretical model, this article proposes that the EU has instead entered a Regulatory Mercantilist phase where it seeks to reassert its control over cyberspace, impose digital borders, accumulate data wealth and reduce its dependence on external private sector actors whose values may not reflect those of the EU order. A new approach to cybersecurity is emerging, in which the non-EU private sector can be perceived as much of a threat as foreign powers, and from whom digital sovereignty must be secured.

Introduction

As the editorial for this special issue indicates, concerns over the EU's security are an element of its turn to a sovereignty-based discourse. Cybersecurity policy in the EU is developing in a time of perceived shifts in the threat landscape, in which those posing threats to the EU's digital security are not only state actors and organised crime networks, but also the private providers of much of the technological infrastructure on which the EU relies. Indeed, the perception on

[1] Benjamin Farrand is Reader in Law and Emerging Technologies at Newcastle University. He is also Director of Education in the Newcastle Law School, and Law & Governance lead in the Newcastle University Centre of Excellence in Cybersecurity and Resilience.

[2] Helena Carrapico is Jean Monnet Chair and Associate Professor in International Relations and Criminology at Northumbria University. She is also co-Director of Research for the Social Sciences Department.

the part of the EU is that its overreliance upon foreign-owned or operated technology originating in the US and China are cybersecurity threats in their own right. Digital sovereignty is, as it relates to cybersecurity, 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. What then, does digital sovereignty mean for public-private relations in the field of cybersecurity?

The development of EU cybersecurity policy can be understood in terms of 'Regulatory Capitalism' as a form of governance; as the infrastructure and services provided online are done so broadly by the private sector, their active engagement in guaranteeing security was both historically necessary and desirable. Sharing a mutual interest in ensuring the resilience and continuity of service provision, the private sector increasingly became involved in both 'rowing' (or implementing) cybersecurity provision, and then 'steering' (or devising) that provision. However, over the past five years, these relations with the private sector are being reconceptualised. As international relations become more acrimonious, with increased tensions between states and protectionism becoming commonplace, questions regarding the role of technology providers in contributing to insecurity are being raised. This article argues that in order to best understand public-private relations in the field of cybersecurity governance in the time of digital sovereignty, it is necessary to consider the EU's changing approach to cooperation with the private sector. More specifically, cybersecurity governance is moving from a field typified by 'Regulatory Capitalism', in which the private sector holds a privileged coregulatory position within the Commission's regulatory efforts, to one of 'Regulatory Mercantilism' in which the Commission positions the private sector as something to be overseen and controlled. Regulatory Mercantilism is characterised by an increased desire for active control over regulatory design, building a secure territory through reducing external dependencies, accumulating data resources within that territory, and using this accumulation of digital power to set the norms both internally and, it is hoped, externally. In this governance mode, the 'domestic' private sector maintains a position of active cooperation in regulation through both 'steering' and 'rowing'; the 'foreign' private sector, however, as both economic competitors and potential agents of other states, are no longer part of the solution to cybersecurity threats, but presented as threats in and of themselves.

The article is structured as follows: section one of the article expands upon the concept of digital sovereignty and the conceptualisation of the private sector within the European

Commission's discourse, before providing an overview of the concept of Regulatory Capitalism, why its current form no longer effectively explains the governance of cybersecurity in the EU, and how the concept of Regulatory Mercantilism can address these deficiencies. Section two of the article provides the historical context to the current governance approach informed by digital sovereignty, by exploring the origins of EU cybersecurity policy and the role of the private sector as a collective actor in both 'steering' and 'rowing' cybersecurity policy. It discusses how concerns over the fundamental values of the EU became layered over the economic goals that served as the basis for EU cybersecurity policy, and how increased concerns over 'hybrid threats' led to a reformulation of EU approaches to digital security that necessitated a reassessment of its engagement with the private sector. Section three highlights the increased concerns over control, territoriality and comparative data wealth on the part of the EU, and how these concerns have served to shape a cybersecurity policy in which EU-based technology firms are trusted regulatory partners, whereas dependence on non-EU based firms is considered as weakening security. Regulatory Mercantilism as a theory of governance is applied in order to help us better understand the EU's turn to a more *dirigiste* form of cybersecurity policy, in which active control and steering of the future of technological innovation is deemed central to ensuring the security of the EU as a regulatory actor.

It is important to state at this juncture that this article focuses upon the efforts of the EU, and in particular the European Commission, in promoting a regulatory shift, rather than upon the responses of the private sector to these shifts, or whether the move to regulatory mercantilism in cybersecurity is likely to be successful in achieving its security goals. It therefore does not seek to argue that the European Commission's economic policies are now those of a mercantilist actor.[3] It is intended that this article works as an exploration of a changing Commission discourse and policy platform, with future works by the authors then exploring how private sector actors are responding to these shifts.

1-Reflections on the intersection between digital sovereignty and the private sector in EU cybersecurity

[3] Mercantilism itself is a varied and variable form of political economy, with varieties not unlike those of capitalism - see (Helleiner, 2021) for an excellent analysis of these myriad approaches.

The Conceptualisation of the Private Sector within the EU's Discourse on Digital Sovereignty and Cybersecurity

As discussed in the editorial of this special issue, we have been able to observe over the past few years the emergence of a EU discourse highlighting the need to strengthen the Union's digital sovereignty in order to face the economic and security challenges of the 21st century (von der Leyen, 2021a). Although the digital sovereignty rhetoric constitutes a new feature within the wider EU discourse, the EU can be seen as a newcomer in a debate that goes back to the end of the 1990s, which highlights the challenges faced by States in controlling and securing cyberspace activities, and which involves not only key world actors such as the United States, China and Russia, but also Member States (namely France and Germany) (Couture and Toupin, 2019; Thumfart, forthcoming). The EU's discourse is constructed in the context of this historical debate, not only through the Europeanisation of national Member State ideas on digital sovereignty, but also reactively by responding to external developments, such as the Snowden revelations (De Hert and Thumfart, 2018; Pohle, 2020). The result is formulated as a vision of the EU's direction of travel that highlights concerns with its degree of dependence on and lack of control over non-EU digital infrastructures, services and content providers, its reduced competitiveness, market presence, and innovation, and its capacity to guarantee a high level of cybersecurity for EU citizens, companies, and infrastructures (Celeste, 2021; Moerel and Timmers, 2021). More than a set of concerns, the EU's discourse reflects the anxieties of an integration project in the context of the 21st century, expresses what kind of security and economic actor it wishes to become, and presents the achieving of sovereignty as the key to realising its potential (Editorial, this issue; von der Leyen, 2021). As discussed by several authors in this issue, however, such vision may come across as surprising given that 1) the concept of sovereignty has traditionally been associated with State power and territoriality, revealing a lack of precedent for a claim to sovereignty from a supranational organisation (Bellanova et Al., Barrinha and Christou, Monsees and Lambach, Bellanova and Glouftsios, this issue); and 2) as understood in the Western World, cyberspace corresponds to a borderless domain that is governed in a cooperative fashion through a range of State and non-State actors, making it particularly difficult for any one entity to exercise control (Mueller, 2020). This is particularly true of the private sector, given that a substantial part of critical information infrastructure are owned and managed by public-private partnerships (Carrapico and Farrand, 2017). The remainder of this section wishes to further explore this second point, namely what

the EU understands by sovereignty in the context of a shared governance field, and how it perceives the role of private actors in enabling it to achieve such sovereignty.

When analysing the corpus of policy documents and speeches produced by different EU institutions that mention digital sovereignty, it becomes quickly apparent that, although no specific definition is readily offered, the concept is equated with the 'ability to act independently in the digital world' (Madiega, 2020, p. 1). This idea of independence, however, is not understood as excluding the private sector, but rather as relying on it to achieve every measure of success. More specifically, four main understandings of the private sector and its centrality emerge within the EU digital sovereignty discourse: 1) as the driver of innovation, enabling the EU to develop new products and services that will improve the competitiveness of the EU economy, as well as EU citizens' quality of life (European Commission, 2020a; von der Leyen, 2021b); 2) as a trusted like-minded partner that, not only shares the EU's values of openness, democracy, rule of law, and fundamental rights, complying with its ethical rules and legislation, but also contributes towards developing EU digital norms and high standards and towards their exporting beyond EU borders. On this point, the EU is increasingly making a distinction between EU-based companies, which adhere to its values, and non-EU large corporations, which are seen as being as following US or Chinese norms (European Commission, 2021a); 3) as the guarantor of cybersecurity, which creates a safer digital environment for EU infrastructures and EU citizens. The private sector is seen as being ideally positioned to create safe products that are trusted by citizens, to protect citizens' data from foreign interference through cyber resilience, and to have access to privileged information on the most recent security developments on the ground (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020; von der Leyen, 2021c); and 4) as a funding partner, whose economic and know-how investment will enable the EU's digital sovereignty plans to come to fruition (European Commission, 2021a).

These four elements are understood as being intimately linked in creating the necessary conditions for EU digital sovereignty to develop: businesses create a safe environment that ensures the integrity and resilience of infrastructure, which then allows for them to serve as a motor of innovation, so that the economy can expand in line with EU values and norms and the EU's dependency on other parts of the world is reduced (European Commission, 2020b).

Conceptualising the role of the private sector within the EU digital sovereignty discourse and EU Cybersecurity

In order to understand the role that the private sector plays in the introduction of the concept of digital sovereignty within EU Cybersecurity, the article builds upon previous work by the authors undertaken in the context of the 'regulatory capitalism' framework (Carrapico and Farrand, 2021, 2020). This Political Economy- based theoretical lens explores the participation of the private sector in providing and regulating public services by offering a historical perspective on the way the division of labour between the public and private actors has evolved in Europe and the United States (Braithwaite, 2005; Levi-Faur, 2005). By asking who was responsible for creating policies and making policy decisions ('steering'), and for implementing such decisions ('rowing'), Regulatory Capitalism offers an analysis of the way the responsibility for rowing, and at times, steering, shifted from the public sector to the private one. In doing so, it offers a convincing explanation for the change in understanding of the role of private actors over the course of the last two centuries and how it was shaped by Neoliberal thought. More specifically, it develops the idea that the private sector was perceived as better placed to achieve economic and societal development because it was considered to be more efficient, stable, and apolitical (Harvey, 2007). As can be seen in table 1, Regulatory Capitalism identifies four time periods in the governance of public services: 1) Laissez-Faire Capitalism phase (1800s-1930s), characterised by the 'steering' and the 'rowing' being the responsibility solely of the private sector; 2) the Welfare Capitalism phase (1940s-1970s), where the State becomes responsible both for the 'steering', namely the organisation and planning of the economic activity, and the 'rowing'. Private sector activity continues to take place throughout this phase, although relations between public and private actors become clearly hierarchical; 3) the Regulatory Capitalism phase (1980s-2010s), where the public sector continues to 'steer', but deregulatory (or liberalisation) and re-regulation approaches enable the private sector to become responsible for a larger proportion of the provision of public goods and services; and 4) Networked Regulatory Capitalism (2010s onwards), characterised by less hierarchical relations and the emergence of the private sector as one of the 'steering' actors. In this phase, the private sector is understood not only as being best placed to provide the goods and services, but also to regulate them, either through forms of self-regulation or by taking part in decision-making bodies. In these capacities, the private sector has been able to shape regulatory norms, as well as to give them effect. Networked regulatory capitalism can be considered as having an element of 'selective' relations with private sector actors, in which some are considered as

trusted partners capable of 'steering' as well as 'rowing', whereas some less trusted actors are relegated to a 'rowing' position.

	Laissez Faire capitalism (1800s-1930s)	Welfare Capitalism (1940s-1970s)	Regulatory Capitalism (1980s-2010s)	Networked Regulatory Capitalism
Steering	Business	State	State and Agencies	State, Agencies, (Business)
Rowing	Business	State	Business	Business
Levels of Trust	N/A	Low	Medium	Variable

Table 1: Source: Adaptation of Levi-Faur (2005) and Braithwaite (2005).

However, as subsequent sections of this paper will demonstrate, it is felt that Regulatory Capitalism, as currently understood, cannot adequately explain the sovereignty turn in cybersecurity governance. As discussed in Carrapico and Farrand (2021), the role of the private sector in both 'rowing' and 'steering' is dependent upon relations of trust and an understanding of shared values and interests. With the rise of hybrid threats in the digital sphere, the spread of disinformation and increased concern on the part of European institutions that large social media platforms do not share the same interests and values as the EU, these trust relations are breaking down, as is the willingness to have these private sector actors involved in the EU's regulatory structures. Instead, the authors propose that a new dynamic has developed in this space which, as a related regulatory phenomenon, can be conceptualised as 'Regulatory Mercantilism'. As with Regulatory Capitalism as a form of governance, Regulatory Mercantilism does not seek to embed *all* aspects of mercantile thought but shares distinct characteristics with them. Mercantilism can be defined as the pursuit of 'stateness' which is concerned with 'the protection of the state and the pursuit of the "national interest"' (Hettne, 1993, p. 213). For Gilpin, there is a tension between 'state' and 'market', as 'the logic of the market is to locate economic activities where they are most productive and profitable; the logic of the state is to capture and control the process of economic growth and capital accumulation' (1987, p. 11). Mercantilism sought to reconcile this tension in favour of the state, with control

of the economy to serve the interests of the state. As Nachbar argues, what 'most clearly separated mercantilism from the capitalist economic systems that followed was its emphasis on collective, rather than individual, wealth' (Nachbar, 2005, p. 1318). Sharing similarities with Realist international relations, Mercantilism equates political power with wealth, and wealth with political power. For this reason, Mercantilism was believed to prioritise a positive trade balance, in which imports were restricted and exports were promoted (Allen, 1991). Wealth was framed in terms of control over money and coinage (Herlitz, 1964), the accumulation of which grew the power of the state, promoting the security of the state in the face of external threats (Conti, 2018). For Helleiner, the commonality to different mercantilist approaches classified as neomercantilist was in 'the belief in the need for strategic trade protectionism and other forms of government economic activism to promote state wealth and power in the post-Smithian age' (2021, p. 4). In this respect, Mercantilism as a philosophy of governance was something of a responsive understanding of state relations, and very much a product of its time (Barth, 2016). Bearing this in mind, then, why is Mercantilism useful when considering digital sovereignty?

The EU can be argued to have become less market liberal in approach to economic policy issues after the Global Financial Crisis. As Youngs argues, the EU is increasingly 'married to an apparent assumption that state-centric multi-polarity is emerging as the defining organisational logic of the international order' (2013, p. 477). This is not necessarily a faulty assumption on the part of the EU, as evidenced by the past several years of worsening state relations; nations and regions are becoming increasingly insular and nationalistic, with a rise in protectionist economic policies (Hesse, 2021), challenges to the legitimacy (Petersmann, 2020) and functioning (Pauwelyn, 2019) of liberal international organisations such as the World Trade Organization (WTO), and indeed, the 'anti-system' driven move by the UK to withdraw from the EU (Hopkin, 2017, see also 2020). Indeed, in a world seemingly preoccupied with Realist conceptions of sovereignty, and where states see each other as potential threats and competitors rather than partners in international cooperation, the EU's own sovereignty turn is not so surprising. Trade in particular is no longer seen as a net positive, in which all WTO members willingly participate, but instead as a source of conflict and power imbalances, to the detriment of multilateral approaches to problems (MacIsaac and Duclos, 2020). These rising tensions, and the impact they have upon the perception of EU vulnerability to exogenous threats, provide context for the increased concerns over sovereignty, including of a digital form, and for the move to Regulatory Mercantilism as a means of governing

perceived cybersecurity threats. Regulatory Mercantilism can be understood as an adaptation of 'selective' Regulatory Capitalism, in which the private sector is subject to the regulatory will of the state, rather than cooperating as 'equal partner' in that regulatory structuring. It shares similarities with Regulatory Capitalism insofar as the State takes on a larger role in 'steering', along with selected private partners, with other businesses relegated to 'rowing' positions placed on variables in trust relations. However, where it diverges is in the level of desired control over governance, and the emphasis on territorial location as a key dimension of trust. Regulatory Mercantilism has three distinct characteristics: the first is an increasingly *dirigiste* approach to governance, in which the state (in this case, the EU) takes a more active 'state-building' role in setting regulatory frameworks and exerting control on the basis of an explicit security logic; the second is a protectionist dimension to governance, which seeks a regulatory 'balance of trade', in which regulatory exports are desirable and regulatory imports undesirable; and the third is that the accumulation of wealth (broadly defined) within the state is seen as beneficial in strengthening the regulatory power of that state.

	Laissez Faire capitalism (1800s-1930s)	Welfare Capitalism (1940s-1970s)	Regulatory Capitalism (1980s-2010s)	Regulatory Mercantilism (late 2010s-present)
Steering	Business	State	State and Agencies	State, Agencies, 'Internal' Business Partners
Rowing	Business	State	Business	'External' Business
Levels of Trust	N/A	Low	Medium	Variable based on territoriality
Vulnerability perception	N/A	Low	Low	High

Table 2: Source: Adaptation of Levi-Faur (2005) and Braithwaite (2005), modified to incorporate Regulatory Mercantilism.

2- The evolution of private sector cooperation in cybersecurity governance: from regulatory subjects to trusted partners

The Commission's turn to 'sovereignty' has not resulted in a concomitant shift in cybersecurity policies and EU relations with the private sector. Instead, the role of the private sector in cybersecurity policy is characterised by significant levels of continuity, with changes in the field largely being gradual. In order to evidence this, this section of the article expands upon the origins of the EU's approach to the Internet generally, which in turn has informed its specific cybersecurity policies. The challenges posed by new technologies are characterised as ultimately being problems of the EU's weak competitive position compared to other international powers, best tackled through setting regulatory frameworks in order to facilitate increased competition and promote the development of European private initiatives. This has created governance practices that have gone on to set the parameters for European cybersecurity, in which the private sector is expected to take an active role in promoting Europe's cybersecurity interests, predominantly through market-based approaches (Farrand, forthcoming).

Setting the framework: information technology for market competitiveness

The EU's understanding of the problems posed by a weak competitive position internationally, which has in turn served to shape the EU's approach to Internet regulation, can be traced back to the late 1970s, with the Commission's Communication on the challenges of new information technologies (European Commission, 1979). In this Communication, the Commission argued that in the context of the 'difficult' transition away from economies based on coal and steel, there was a need to pursue a model of growth based on engagement with 'new electronic technologies' (1979, p. 1). The technologies identified ranged from satellites and fibre-optic cables, through to (somewhat astonishingly, demonstrating that many of these concerns are not necessarily 'new') artificial intelligences, or AI (1979, p. 2). The main problem, according to the Commission, was the EU's weak competitive advantage – European-owned computer companies were identified as representing only 16% of the world market, compared with 73% based in the US. Furthermore, European companies imported over 80% of its used integrated circuits, and the EU was facing fierce competition from the US and Japan, which were considered better placed to take advantage of the electronic revolution (European Commission,

1979, pp. 2–5). If the proposed problems were market-based in nature, then so too were the proposed solutions; increasing competition through setting regulatory frameworks would facilitate the growth of European-based information technology companies, creating effective market conditions for these companies to operate within, and fostering industrial and user collaborations to maximise the benefits of these developments (1979, pp. 5–8). In doing so the EU could oversee the 'creation of a common information area [which] will depend primarily on private sector investment. It is therefore essential to create a legal environment which will stimulate the development of such investments' (European Commission, 1979, p. 14). In other words, it would be through public-private partnership that these solutions could be realised, with the public sector 'steering' technological development, and a newly empowered private sector performing the 'rowing' to make those developments happen. As such, this initial positioning effectively mirrors the initial position of regulatory capitalism in the 1980s.

This theme of public 'steering' and private 'rowing' runs through the two key Communications that identify the themes for the EU's understanding of the policy challenges it faced through rapid developments in communications technologies in the 1990s and outline the EU's position on the Information Society: the Communication on Growth and Competitiveness (European Commission, 1993) and the Bangemann Report (European Commission and Bangemann Group, 1994). Identifying a lack of competitiveness on the part of the European economy in the 1993 Communication, the Commission concluded that the best way of ensuring economic growth in order to 'catch up' to the US and Japan would be through creating a legal environment that would stimulate private sector initiatives in the field of information technology (1993, p. 112). The 1994 Bangemann report, identified as being highly influential in the development of the EU's approach to Internet-related regulation (see for example Christou and Simpson, 2006), reinforced this approach to Internet policy-making, arguing that the development of the European Information Society 'should be entrusted to the private sector and to market forces' with the EU setting the regulatory framework in which this would happen (European Commission and Bangemann Group, 1994, p. 34). The E-Commerce Directive (Directive 2000/31/EC, 2000), the EU's first regulatory initiative directly relating to the role of private sector actors present on the Internet, was the legislative result of this public-private approach. Articles 12-15 of the Directive set up the framework for intermediary liability for the use of the information society services they provided, granting a general immunity from liability insofar as these private sector actors moved judiciously to remove any illegal or right infringing content cached or hosted on their services that was brought to their attention. While

not overtly concerned with issues of cybersecurity, but instead the mitigation of traditional offences moving from the offline to online environments, these principles nevertheless established the basis for private sector cooperation that would begin to incorporate steering as well as rowing.

'European' cybersecurity: layering values over markets and sovereignty in all but name

When cybersecurity moved from being an implicit aspect of EU information technology policy to its own dedicated area and field of activity within the Area of Freedom, Security and Justice in the early 2010s (Carrapico and Farrand, 2017; Fahey, 2014), the private sector was privileged with a 'steering and rowing' position within the cybersecurity framework. This position was based in the understanding that the private sector was best placed operationally to undertake these activities, possessing the necessary expertise to devise the protocols and procedures for guaranteeing cybersecurity. Furthermore, there was understanding on the part of the public sector that private sector cooperation was incentivised due to shared risk in the event that cyberattacks were successful (Ballou et al., 2016; Christensen and Petersen, 2017). Again, however, the approach to cybersecurity was predominantly born out of economic concerns, in this instance the impact on the European economy of the global financial crisis and a perception that the EU was in a weak competitive position globally (European Commission, 2010a, p. 5). Contemporary approaches therefore dictated that the appropriate response to these problems was the establishment of new regulatory frameworks in order to facilitate competition in the European digital space. In terms of cybersecurity specifically, while there was acknowledgment that cyberattacks could be politically motivated, the main focus of these policies was in heightening trust in the use of the Internet for the purposes of commerce (European Commission, 2010a, pp. 16–17). The resulting initiatives culminated in the establishment of the European Cyber Crime Centre (EC3) and the European Network Information Security Agency (ENISA, now known as the EU Agency for Cybersecurity) (European Commission, 2010b), with ENISA functioning as a centre for public-private collaboration in developing best practices and standards for cybersecurity provision. In 2013, the EU's cybersecurity approach was further formalised in the Cybersecurity Strategy (European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, 2013). In this document, we can see an emerging layering process through the explicit references to the 'core values' of the EU such as privacy and freedom of expression being added to the existing economic justifications for cybersecurity action (2013, pp. 3–4),

albeit on the basis that 'the private sector should continue to play a leading role' (2013, p. 3). The private sector, at least at this point in time, was understood to share in these values, and therefore could continue to act as a trusted partner in these regulatory activities.

Interestingly, it is here in the context of a layering of 'values' over 'markets' in European cybersecurity that we see two of the only references to 'sovereignty' in the context of digital policies prior to its mainstreaming by the von der Leyen Commission. In a 2010 Impact Assessment on the Proposal for a Regulation on ENISA, there is a reference to a response from an academic institution claiming that enforcing the rule of law on the Internet could help the 'state to regain its "digital sovereignty"' (European Commission, 2010c, p. 93). In 2017, an Impact Assessment accompanying proposals to expand ENISA's competences and develop a cybersecurity certification scheme (known as the Cybersecurity Act) included a case study from the German Ministry of the Interior that 'European digital security is challenged on other fronts [including the need to defend infrastructure from cyberattacks, develop a European digital security industry and determine how data should be protected in Europe], requiring a collective ambition to guarantee Europe's digital sovereignty' (European Commission, 2017, p. 166). What explains this shift to the use of sovereignty as a rationale for EU cybersecurity policy? In no small part, a security spillover relating to geopolitical concerns such as the actions of Russia in the Ukraine, as well as online, and the expanding influence of China was coupled with an increasing sense that the private sector as a general category of actor may not necessarily share the 'values' of the EU, resulting in faltering trust relations (Carrapico and Farrand, 2021). In terms of geopolitics, the acknowledgment by the EU that the use of the Internet could facilitate hybrid threats against both information and the infrastructure supporting it by State as well as non-State actors led to the fostering of a cybersecurity approach where cybersecurity became an explicit security focus within the AFSJ rather than predominantly as the result of economic concerns in the Internal Market (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016).

With regard to trust in the private sector, concerns over the use of private user data by companies such as Facebook in the light of the Snowden revelations (Steiger et al., 2017), which became compounded with the sense that US-based social media platforms were increasingly being used to spread disinformation and destabilise European democracies, both in the context of the UK's referendum on EU membership, as well as national elections

(Morgan, 2018; Hameleers et al., 2020). This resulted in the implementation of the General Data Protection Regulation, in which significant regulatory pressure was brought to bear on the private sector uses of personal data, reducing the 'steering' capacity of the private sector and imposing strong 'rowing' obligations on them, as well as the adoption of codes of practice for social media platforms to mitigate the impacts of disinformation being spread through their platforms (European Commission, 2018a, 2018b). Further indicating a change of approach to engagement with the private sector, the Commission has reiterated that if they believed that social media platforms were not acting to tackle these challenges, stricter 'top-down' actions could follow (European Commission, 2019). In comparison, private sector actors working on developing security solutions maintained a privileged 'steering' position, through devising and implementing best practice standards and providing cybersecurity certifications under Regulation 2019/881. This period can be categorised as one of in which we see clearer indications of selectiveness in Networked Regulatory Capitalism, where private actors perceived to share the values and/or interests of the EU remain trusted nodes in a regulatory structure, but those who are not seen to share those values or interests are instead tasked with rowing rather than steering in the realisation of cybersecurity goals (Carrapico and Farrand, 2021).

It is worth nothing that these discussions of the increasing cybersecurity threat and the changing relationship with the private sector were not couched explicitly in digital sovereignty terms. Nevertheless, through these measures, we see the origins of a conceptualisation of cybersecurity as possessing a sovereignty dimension, indicating that the sovereignty turn did not begin with the von der Leyen Commission but was being developed earlier. However, it is from 2019 onwards that 'digital sovereignty' is constituted as a specific, explicit policy of the Commission, with implications for private sector cybersecurity relations. In the next section of this article, we shall explore how this selective Networked Regulatory Capitalism governance model is being adapted by the emphasis on digital sovereignty, to the extent that we could consider it reflecting a move to a form of Regulatory Mercantilism over cybersecurity.

3- Shaping Europe's Digital Sovereignty: from Regulatory Capitalism to Regulatory Mercantilism?

In the political guidelines issued as part of von der Leyen's Commission President candidature, von der Leyen made it clear that 'digital sovereignty' comprised one of her key policy

priorities, securing the creation of a Europe 'fit for the digital age […] within safe and ethical boundaries' (2019, p. 13). Her political guidelines acknowledged the advanced state of the technology industry, but considered that it was 'not too late to achieve technological sovereignty in some critical technology areas' (von der Leyen, 2019, p. 13). Sovereignty in the context of this document referred to the ability to choose a 'European way' for digital technologies, balancing the opportunities presented by the use of data with privacy, security, safety and ethical standards (von der Leyen, 2019, p. 13). These political guidelines were then crystalised in the Communication on Shaping Europe's Digital Future, published shortly before awareness of the COVID-19 pandemic fully materialised in the EU (European Commission, 2020b). Choice, conceptualised as the ability to choose the regulatory frameworks for private sector action, remains a central element in this conceptualisation of sovereignty:

> Sovereignty starts from ensuring the integrity and resilience of *our* data infrastructure, networks and communications. It requires creating the right conditions for Europe to develop and deploy *its own* key capacities, thereby *reducing our dependency on other parts of the globe for the most crucial technologies*. Europe's ability to *define its own rules and values* in the digital age will be reinforced by such capacities (European Commission, 2020b, p. 3). [Emphasis added]

Here we begin to see elements of a Regulatory Mercantilist approach to cybersecurity governance, in which a clear binary is created between 'our' EU-based infrastructure and technologies and the EU's 'own' security, resilience and values, and those of the rest of the globe. Dependency on technologies from outside the EU is discursively framed as weakening European security, with the development of these technologies *within* the EU contributing to increased strength and influence. While the policy proposals are not necessarily distinct from those of the 1970s and 1980s, the discourse is, insofar as it focuses less on pure economic competition concerns, and more on explicit security threats with the potential to destabilise the EU. As discussed earlier, the infrastructure, networks and communications systems (including online platforms as well as physical architecture) are privately owned and operated. Reducing dependency on 'other parts of the globe', as the Communication puts it, necessitates reducing dependency on the non-EU providers of that infrastructure, networks and communications, as well as restricting the likelihood of regulatory 'imports'. This desire to reduce dependency does not only relate to US-based companies perceived to pose informational threats to the EU, such as Facebook or Google, but also Chinese firms such as Huawei, which is perceived as

presenting potential threats to network infrastructure. It is this element of 'inside' and 'outside', or 'EU' and 'foreign' that leads us to argue that the current trend in 'selective' regulatory capitalism entails a move to a form of Regulatory Mercantilism. Rather than working in open cooperation with all private stakeholders involved in both 'rowing' and 'steering' in cybersecurity policy, the emphasis of digital sovereignty-focused cybersecurity entails a move to *dirigiste* control in the European interest, to protect the region from external threats. These threats include non-EU private sector actors as much as it does third states. In terms of policy, this entails much more active 'steering' from the public sector, with 'rowing' performed by the private sector. What 'steering' may be undertaken by the private sector is largely dependent upon alignment with EU values, with trust heavily dependent on geographical location.

Sovereignty in cybersecurity: new language, old policies?

Assessment of the cybersecurity policies born out the Shaping Europe's Digital Future initiative leads to the conclusion that while Shaping Europe's Digital Future does not represent a shift in terms of the content of policies and actions, it does represent a significant reconceptualisation of relations between private sectors operators and the Commission, in which being a regulatory partner entrusted with steering those policies and actions is predicated upon being EU-based. A key indicator in the document itself comes from the above-cited paragraph, where it is stated that this sovereignty is facilitated through creating the right conditions for Europe to develop its *own* capacities, its *own* private sector champions (a word associated with state planning and *dirigisme* in economic affairs), and indeed, defining its *own* rules and values. The agenda demonstrates a clear desire for more active control over these processes and the selection of private sector partners, rather than allowing the private sector as a general category to make these decisions through purely market-based decisions. This can be evidenced by the policy proposals put forward by the Commission following this Communication, in which digital or technological sovereignty are explicitly mentioned.

The changing relations between foreign-based Big Tech and EU cybersecurity aims is made readily apparent in the Cybersecurity Strategy for the Digital Decade published in December 2020 (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020). The EU refers to a 'threat landscape compounded by geopolitical tensions […] and over control of technologies' (2020, p. 1), framing its response in terms of 'thinking global, acting European' (2020, p. 4). In its three-pronged approach of deploying

regulatory, investment and policy instruments intended to 'shield its people, businesses and institutions from cyber threats' (2020, p. 4), the Joint Communication states that the first pillar of its strategy is 'resilience, technological sovereignty and leadership' (2020, p. 4). The actions identified under this pillar are broad in scope, including revisiting the Network and Information Systems Directive (Directive 2016/1148, 2016, the NIS Directive), introducing regulatory measures to create an 'Internet of Secured Things', securing 5G and other new communications technologies, and working to develop effective public-private partnerships through the establishment of bodies such as the Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs), AI-enabled Security Operation Centres (2020, pp. 5–13). It is worth noting that the only reference to sovereignty in these proposals relates to the establishment of the ECCC and the CNN, which are encouraged to develop 'the EU's technological sovereignty in cybersecurity' (2020, p. 11).

Interestingly, a Proposal for a Regulation establishing the ECCC and the CNN was initially made in 2018, emphasising the importance of cybersecurity coordination in Europe in order to secure its Digital Single Market (European Commission, 2018c, p. 1). Although it did not mention sovereignty in any way, the document implicitly makes the connection between sovereignty and the development of public-private partnerships, tasking itself with providing a regulatory environment that facilitates the growth of these initiatives. This can be contextualised in light of the September 2020 Strategic Foresight Report (2020c), where the Commission states that the EU possesses certain vulnerabilities, particularly in terms of its cybersecurity. This report identifies the 'rapidly escalating US-China technological confrontation' (2020c, p. 30) as a key source of vulnerability, 'reinforcing the need for the EU to pursue its technological sovereignty agenda and strengthen its key digital capacities' (2020c, p. 31). The role of sovereignty as a discursive framing for cybersecurity appears to be serving as an instigator for action in which 'domestic' private-sector actors are privileged regulatory nodes; the Report on the Cybersecurity Strategy published in June 2021 reiterates that 'political and economic development requires technological sovereignty and a global, open and secure cyberspace, grounded in the rule of law and respect for human rights and fundamental freedoms' (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2021, p. 1). This serves as the basis for a range of regulatory interventions in cybersecurity, including proposals for a revised NIS Directive- 'NIS2' (European Commission, 2020d), a Directive on critical entities (European Commission, 2020e), and a Regulation on financial sector resilience (European Commission, 2020f). None of these

proposals explicitly mentions sovereignty, but are all categorised in their explanatory memoranda as falling within the remit of the Shaping Europe's Digital Future agenda, seeking to provide regulatory instruction to private sector operators in the EU regarding standards of best practice to implement in order to ensure effective cybersecurity provision. Sovereignty in this context therefore constitutes the ability of the EU to lay out these regulatory standards, despite not necessarily having sovereignty over the networks and information system infrastructure. Regulatory Mercantilism can be seen in the framing of these regulatory concerns as intended to mitigate external threats, an increased desire for control, and the fostering of 'domestic' private-sector initiatives and trust relations based on the sharing of European values. If we go beyond the 'macro' level of cybersecurity to focus on sector-specific proposals, the re-conceptualisation of the relations between public and private sectors in terms of sovereignty becomes even clearer.

Digital Sovereignty in All Things: Cybersecurity as a transversal concern

One of the first publications drawing from Shaping Europe's Digital Future was the White Paper on AI released in February 2020 (European Commission, 2020a), which states that the measures proposed will 'increase Europe's technological sovereignty in key-enabling technologies and infrastructures for the data economy' (2020a, p. 3). The main problem identified in this document is that while the EU is 'well-placed to benefit from the potential of AI' (2020a, p. 3), and more than 50% of manufacturers in Europe deploy AI (2020a, p. 4), the majority of the AI solutions relied upon are both financed and developed outside of the EU, which at €3.2 billion in investment in 2016 trailed investment in North America at €12.1 billion and €6.5 billion in Asia (2020a, p. 4). Concerns over sovereignty in this field of research are centred on this comparatively weak position of international competition, with acknowledgement that the application of the data and algorithms that form 'AI' can have significant security implications, including in the field of cyber-security (2020a, p. 10). The proposed actions in order to mitigate these threats demonstrate a mercantilist turn to selective regulatory capitalism; measures to be pursued included providing the conditions for markets for European-based AI research and development to take place, through academic funding projects and skills development, providing funding for Small and Medium Size Enterprises (SMEs) and forming public-private partnerships with European companies to develop AI solutions (2020a, pp. 5–7). In terms of proposed regulatory frameworks, the Commission concluded that regulation was needed that would ensure the protection of EU principles and

values, and 'should be consistent with other actions to promote Europe's innovation capacity and competitiveness […] create a frictionless internal market for the further development and uptake of AI' (European Commission, 2020a, p. 10). The resulting Proposal for a Regulation published in April 2021 (European Commission, 2021b) largely mirrors this approach, referring to ensuring Europe's digital sovereignty in its explanatory memorandum (2021b, p. 6) and proposing a regulatory framework that would involve greater standard setting in areas of AI development considered more high-risk (covered in Title III of the proposed Regulation), with private sector providers of lower-risk applications bound only by voluntary codes of conduct (Title IX of the proposed Regulation). The concept of digital sovereignty proposed in this Regulation largely draws from the existing governance approaches used in other fields of EU activity and reinforces it as a right to set regulatory standards, through providing the conditions for European markets to flourish, while providing a regulatory framework. As the Commission put it in the accompanying Impact Assessment, this digital sovereignty could be threatened due to the fact that 'AI-driven products and services from foreign countries might not completely comply with European values and/or legislation or they might even pose security risks […] tech sovereignty will also facilitate the development and leverage of […the] regulatory power to shape global rules and standards on AI' (European Commission, 2021c, pp. 26–27). In other words, working with trusted EU-based private sector partners allows for the development of standards of practice that can then be 'exported', ensuring a positive regulatory balance in which potential security-threatening imports are reduced, but European values uploaded to the international arena.

Another policy area with specific cybersecurity implications that the Commission has linked to digital sovereignty is that concerning 'data'. Particularly in the cloud storage sector, European private providers lag considerably behind the offerings of US and China-based companies, who are responsible for hosting more than 80% of the world's data (Aktoudianakis, 2020, p. 4). Furthermore, it is estimated that while 92% of the data produced in the West is hosted in the US, only 4% is hosted in the EU (Kalff and Renda, 2019, p. 173). In the February 2020 European strategy for data Communication (2020g), it was made clear that cybersecurity and compliance with EU values is central to the data strategy. Concerns predominantly focused on two main areas of potential insecurity. The first was the market concentration effects apparent in the US characterised by few market players of highly significant size. The second focused on the role of the Chinese state in active digital surveillance coupled with 'a strong control over Big Tech companies over massive amounts of data without sufficient safeguards'

(2020g, p. 3). Again, the proposed solution to these problems is through facilitating EU market activity and fostering competition, guided by a regulatory framework that is intended to ensure that 'by 2030, the EU's share of the data economy – data stored, processed, and put to valuable use in Europe – at least corresponds to its economic weight, not by *fiat* but by choice' (2020g, p. 4). In this respect, data is seen as analogous to wealth – by trying to maximise the amount of this data wealth *within* Europe's borders, it increases its regulatory strength. A proposed Regulation, a first step in implementing the Data Strategy, seeks to facilitate these efforts (European Commission, 2020h). While it does not mention sovereignty explicitly either in its explanatory memorandum or Regulation text, it nevertheless states its purpose is to 'foster the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU' (2020h, p. 1). In other words, facilitating the market conditions through a regulatory intervention is seen as an effective way of ensuring effective competition and promoting the development of EU-based data initiatives, thereby reducing dependence on foreign 'Big Tech'. This is confirmed in the accompanying Impact Assessment where it is stated that the proposed legislation would help the EU in 'maintaining its data sovereignty […and that] such a model is necessary as an alternative to the current business model dominated by Big Tech platforms' (European Commission, 2020i, p. 11). Perhaps as an indication that 'the state' is back in planning and shaping the economy in its interest (as opposed to economics shaping the state), in a recent visit to a chip manufacturer in the Netherlands, President von der Leyen referred to the company as being one of 'our European digital champions […] this company will play a big role in our efforts to make Europe more competitive and more sovereign in the tech sector' (von der Leyen, 2021b). Private sector tech firms can still be trusted partners in European cybersecurity – so long as those firms are European.

Conclusions

The present article contributes to the special issue on *Digital Sovereignty and EU security integration* by exploring how the role of the private sector is represented within the EU's discourse on cybersecurity. It starts by reflecting on the way the concept of sovereignty, whose traditional understanding is equated with territoriality and Statehood, is adapted by the EU to cyberspace activities, which are characterised by an absence of borders, as well as by multistakeholder governance. On this basis, the article proposes that the theoretical lenses of Regulatory Mercantilism are best placed to explain the EU's current concerns over its difficulty

in providing EU citizens with a high level of cybersecurity, which are related to the perceived loss of economic competitiveness, limited capacity to innovate, and high degree of dependence on foreign digital infrastructures and service providers, as well as the resulting shift towards a more dirigiste cybersecurity policy. The article argues that this sovereignty shift has led to a reassessment of public-private relations with EU-based businesses being represented not only as the motor of EU competitiveness and innovation, but also as champions of EU norms and values and as guarantors of EU security.

Given the recent character of the digital sovereignty turn in EU discourse, the present contribution offers a first reflection on the way private actors are being re-conceptualised, but also recognises that there is great potential in this field for further research. In particular, it will be interesting to follow the Commission's efforts to implement its digital sovereignty discourse in the form of initiatives to create a safe online environment, at the same time as the technological landscape evolves rapidly. These initiatives are expected to include the creation of new coordination mechanisms - such as the new Joint Cybersecurity Unit for Member State cooperation and the European Cybersecurity Competence Centres -, the development of common security standards for specific forms of technology, namely 5G and the Internet of Things, and the inclusion of security requirements in public procurement processes and of a compulsory EU-wide cybersecurity certification (Madiega, 2020). The pursuit of these initiatives, under the heading of the EU digital sovereignty agenda, will require the further expansion of the existing public-private partnerships, namely in fields of rapid technological change, such as robotics, artificial intelligence, quantum computing, and cloud solutions. In this context, it will be interesting to analyse in future research, the evolution of trust relations within public-private partnerships, the diversity in the format of these partnerships and their outcomes, the way the private sector is perceiving this digital sovereignty shift, and whether any sites of resistance emerge to the Commission's discourse.

Bibliography

Aktoudianakis, A., 2020. Fostering Europe's Strategic Autonomy: Digital sovereignty for growth, rules and cooperation. European Policy Centre & Konrad Adenauer Stiftung.

Allen, W.R., 1991. Mercantilism, in: Eatwell, J., Milgate, M., Newman, P. (Eds.), The World of Economics, The New Palgrave. Palgrave Macmillan UK, London, pp. 440–448. https://doi.org/10.1007/978-1-349-21315-3_58

Ballou, T., Allen, J., Francis, K., 2016. Hands-off Approach or Effective Partnership? Journal of Information Warfare 15, 44–59.

Barth, J., 2016. Reconstructing Mercantilism: Consensus and Conflict in British Imperial Economy in the Seventeenth and Eighteenth Centuries. The William and Mary Quarterly 73, 257–290. https://doi.org/10.5309/willmaryquar.73.2.0257

Braithwaite, J.B., 2005. Neoliberalism or Regulatory Capitalism (No. Regnet Occasional Paper 5).

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

Carrapico, H., 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 59, 1160–1176.

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

Carrapico, H., Farrand, B., 2017. 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. Crime, Law and Social Change 67, 245–263.

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

Christensen, K.K., Petersen, K.L., 2017. Public–private partnerships on cyber security: a practice of loyalty. International Affairs 93, 1435–1452. https://doi.org/10.1093/ia/iix189

Christou, G., Simpson, S., 2006. The Internet and Public-Private Governance in the European Union. Journal of Public Policy 26, 43–61. https://doi.org/10.2307/4007810

Conti, T.V., 2018. Mercantilism: a materialist approach. Scandinavian Economic History Review 66, 186–200. https://doi.org/10.1080/03585522.2018.1465847

Couture, S., Toupin, S., 2019. What does the notion of "sovereignty" mean when referring to the digital? New Media & Society 21, 2305–2322. https://doi.org/10.1177/1461444819865984

De Hert, P., Thumfart, J., 2018. The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies. The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies, Brussels Privacy Hub Working Papers 4.

Directive 2000/31/EC, 2000. on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

Directive 2016/1148, 2016. concerning Measures for a High Common Level of Security of Network and Information Systems across the Union.

European Commission, 2021a. Proposal for a Decision of the European Parliament and of the Council establishing the 2030 Policy programme 'Path to the Digital Decade'- COM(2021)574 final.

European Commission, 2021b. Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) (No. COM(2021) 206).

European Commission, 2021c. Impact Assessment accompanying the Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) (No. SWD(2021) 84).
European Commission, 2020a. White Paper on Artificial Intelligence: A European approach to excellence and trust (No. COM(2020) 65).
European Commission, 2020b. Shaping Europe's Digital Future.
European Commission, 2020c. 2020 Strategic Foresight Report: Charting the course towards a more resilient Europe (No. COM(2020) 493).
European Commission, 2020d. Proposal for a Directive on measures for a high level of cybersecurity across the Union, repealing Directive 2016/1148 (No. COM(2020) 823).
European Commission, 2020e. Proposal for a Directive on the resilience of critical entities (No. COM(2020) 829).
European Commission, 2020f. Proposal for a Regulation on digital operational resilience for the financial sector (No. COM(2020) 595).
European Commission, 2020g. A European strategy for data (No. COM(2020) 66).
European Commission, 2020h. Proposal for a Regulation on European data governance (No. COM(2020) 767).
European Commission, 2020i. Impact Assessment accompanying the Proposal for a Regulation on European data governance (No. SWD(2020) 295).
European Commission, 2019. Code of Practice on Disinformation: First Annual Reports.
European Commission, 2018a. Tackling online disinformation: a European Approach (No. COM(2018) 236).
European Commission, 2018b. EU Code of Practice on Online Disinformation.
European Commission, 2018c. Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (No. COM(2018) 630).
European Commission, 2017. Impact Assessment accompanying the Proposal on ENISA, the "EU Cybersecurity Agency" and on Information Communication Technology cybersecurity certification (No. SWD(2017) 500).
European Commission, 2010a. A Digital Agenda for Europe (No. COM(2010) 245 final/2). Brussels.
European Commission, 2010b. The EU Internal Security Strategy in Action: five steps towards a more secure Europe (No. COM(2010) 673 final).
European Commission, 2010c. Impact Assessment accompanying the Proposal for a Regulation concerning the European Network and Information Security Agency (No. SEC(2010) 1126).
European Commission, 1993. Growth, competitiveness, employment: The challenges and ways forward into the 21st century (No. COM(93) 700). Brussels.
European Commission, 1979. European society faced with the challenge of new information technologies: a Community response (No. COM(79) 650).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2021. Report on implementation of the EU's Cybersecurity Strategy for the Digital Decade (No. JOIN(2021) 14).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020. The EU's Cybersecurity Strategy for the Digital Decade (No. JOIN(2020) 18).
European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2016. Joint Framework on countering hybrid threats (No. JOIN(2016) 18).

European Commission, Bangemann Group, 1994. Europe and the global information society: Recommendations of the high-level group on the information society to the Corfu European Council (No. S.2/94). Brussels.
European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, 2013. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (No. JOIN(2013) 1). Brussels.
Fahey, E., 2014. The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security. Eur. J. Risk Reg. 5, 46.
Gilpin, R., 1987. The Political Economy of International Relations. Princeton University Press, Princeton, N.J.
Hameleers, M., Powell, T.E., Meer, T.G.L.A.V.D., Bos, L., 2020. A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media. Political Communication 37, 281–301. https://doi.org/10.1080/10584609.2019.1674979
Harvey, D., 2007. Neoliberalism as Creative Destruction. The ANNALS of the American Academy of Political and Social Science 610, 21–44.
Helleiner, E., 2021. The Neomercantilists: A Global Intellectual History. Cornell University Press, Ithaca New York.
Herlitz, L., 1964. The concept of mercantilism. Scandinavian Economic History Review 12, 101–120. https://doi.org/10.1080/03585522.1964.10407639
Hesse, J.-O., 2021. Financial crisis and the recurrence of economic nationalism. J Mod Eur Hist 19, 14–18. https://doi.org/10.1177/1611894420974254
Hettne, B., 1993. Neo-Mercantilism:: The Pursuit of Regionness. Cooperation and Conflict 28, 211–232. https://doi.org/10.1177/0010836793028003001
Hopkin, J., 2020. Anti-System Politics: The Crisis of Market Liberalism in Rich Democracies. OUP USA, New York.
Hopkin, J., 2017. When Polanyi met Farage: Market fundamentalism, economic nationalism, and Britain's exit from the European Union. The British Journal of Politics and International Relations 19, 465–478. https://doi.org/10.1177/1369148117710894
Kalff, D., Renda, A., 2019. Hidden Treasures: Mapping Europe's sources of competitive advantage in doing business. Centre for European Policy Studies, Brussels.
Levi-Faur, D., 2005. The Rise of Regulatory Capitalism: The Global Diffusion of a New Order. The ANNALS of the American Academy of Political and Social Science 598, 12–32. https://doi.org/10.1177/0002716204272590
MacIsaac, S., Duclos, B.C., 2020. Trade and conflict: trends in economic nationalism, unilateralism and protectionism. Canadian Foreign Policy Journal 26, 1–7. https://doi.org/10.1080/11926422.2020.1714682
Madiega, T., 2020. Digital sovereignty for Europe (No. PE 651.992). European Parliamentary Research Service, European Parliament.
Moerel, L., Timmers, P., 2021. Reflections on Digital Sovereignty (SSRN Scholarly Paper No. ID 3772777). Social Science Research Network, Rochester, NY.
Morgan, S., 2018. Fake news, disinformation, manipulation and online tactics to undermine democracy. Journal of Cyber Policy 3, 39–43. https://doi.org/10.1080/23738871.2018.1462395
Mueller, M.L., 2020. Against Sovereignty in Cyberspace. International Studies Review 22, 779–801. https://doi.org/10.1093/isr/viz044
Nachbar, T.B., 2005. Monopoly, Mercantilism, and the Politics of Regulation. Virginia Law Review 91, 1313–1379.
Pauwelyn, J., 2019. WTO Dispute Settlement Post 2019: What to Expect? Journal of International Economic Law 22, 297–321. https://doi.org/10.1093/jiel/jgz024

Petersmann, E.-U., 2020. Economic Disintegration? Political, Economic, and Legal Drivers and the Need for 'Greening Embedded Trade Liberalism.' Journal of International Economic Law 23, 347–370. https://doi.org/10.1093/jiel/jgaa005

Pohle, J., 2020. Digital sovereignty. A new key concept of digital policy in Germany and Europe. Berlin: Konrad-Adenauer-Stiftung.

Steiger, S., Schünemann, W.J., Dimmroth, K., 2017. Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany. Media and Communication 5, 7–16. https://doi.org/10.17645/mac.v5i1.814

Thumfart, J., forthcoming. The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the Covid-crisis 2020/21 as catalytic event, in: Hallinan, D., Leenes, R., de Hert, P. (Eds.), CPDP 2021: Enforcing Rights in a Changing World. Hart Publishing, London.

von der Leyen, U., 2021a. 2021 State of the Union Address by President von der Leyen.

von der Leyen, U., 2021b. Statement by the President on ASML visit [WWW Document]. European Commission - European Commission. URL https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_6050 (accessed 11.24.21).

von der Leyen, U., 2021c. Speech by the President at the Paris Peace Forum [WWW Document]. European Commission - European Commission. URL https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_5977 (accessed 11.24.21).

von der Leyen, U., 2019. A Europe that strives for more: My agenda for Europe.

Youngs, R., 2013. Reviving global Europe. International Politics 50, 475–495. http://dx.doi.org/10.1057/ip.2013.19