In search of digital sovereignty and strategic autonomy: normative power Europe to the test of its geopolitical ambitions

Broeders, D.; Cristiano, F.; Kaminska, M.

JCMS JOURNAL OF COMMON MARKET STUDIES
UACES
JCMS 2023 pp. 1–20 DOI: 10.1111/jcms.13462

In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions

DENNIS BROEDERS,[1] FABIO CRISTIANO[2] and MONICA KAMINSKA[1]
[1]Institute of Security and Global Affairs (ISGA), Leiden University, The Hague [2]Department of History and Art History, Utrecht University, Utrecht

This article analyses the recent use of European Union (EU) terminology of digital sovereignty and strategic autonomy, aiming to identify tensions between policy considerations of fundamental rights, free market principles and geopolitical concerns. These tensions are rooted in the disparity between the EU's considerable economic and regulatory power in digital matters and its limited mandate and capabilities in foreign policy. The article also explores the translation of the notions of digital sovereignty and strategic autonomy into EU policy. It identifies three important trends in the geopoliticisation of the EU agenda on digital technologies: (1) the instrumental use of 'classic' internal market policies to exert geopolitical influence; (2) the imposition of foreign policy imperatives on national markets; and (3) new 'hybrid' digital policies that combine internal market concerns, fundamental rights and geopolitical concerns. Ultimately, digital sovereignty has inherent tensions with the EU's normative power in digital issues and may also result in a strategic cacophony.

Keywords: sovereignty; strategic autonomy; digital policy; cyber security; geopolitics

Introduction

Sovereignty is a troublesome politico-legal concept. It is both the cornerstone of the international (legal) order and fatally under-defined. It is both a divisive and a unifying concept. It has been politically reviled and revered. And whilst Don Herzog (2020, p. ix) attempted to bury the concept once and for all in his recent book *Sovereignty RIP*, Theodore Christakis (2020, p. 1) asserts in reply that 'sovereignty always rises up, zombie-like, for a comeback!'. Cyberspace, famously declared free of sovereignty in its infancy by early cyber-utopians (Barlow 1996), has been one place where sovereignty has become hotly debated again (Demchak and Dombrowski 2013; Mueller 2020), with some authoritarian states such as Russia (Kurowska 2020) and China (Creemers 2020) claiming sovereign rights over their 'national info-sphere'. In more recent years, European states and the European Union (EU) itself have also resorted to the terminology of 'sovereignty' in relation to cyberspace and to digital issues more generally (Timmers 2019; Christakis 2020; Floridi 2020; Pohle 2020; Barrinha and Christou 2022; Broeders 2022). Again, clear definitions have been lacking, but EU officials and policy documents have been using the terms 'digital sovereignty', 'data sovereignty' and 'technological sovereignty' as well as the related term of 'strategic autonomy' with regard to the digital domain. Most fundamentally, references to sovereignty and autonomy 'address' the issue of EU economic competitiveness in the global data economy – highlighting both the risks and the opportunities for the EU economy – as well as the

EU's geopolitical position considering increasing geopolitical tensions, within and beyond cyberspace and digital issues.

The general backdrop of geopolitical rivalry between China and the United States that led to the EU's agenda of establishing itself as a strategically autonomous third actor acquires an extra layer when the competition concerns cyberspace and digital technologies. In the past decade, cyberspace has become thoroughly geopoliticised. Lucas Kello (2017) has characterised the situation as one of 'unpeace', falling short of war but decidedly not peace either. Strategic, low-level, geopolitical competition has become the 'new normal' in the digital domain, which, in Europe, has resulted in a strategic vacuum (Buchanan 2020; Liebetrau 2022). Moreover, states are having trouble figuring out what the 'rules of the road in cyberspace' should be, and there are disagreements about the applicability and boundaries of international legal principles, such as sovereignty, in cyberspace (Delerue 2020). Similarly, states are uncertain about the role and responsibility of large tech companies that are almost quasi-sovereign in their operations and wield vast power as they structure society's information and functioning.

Against this backdrop, it is not surprising that, under the banner of digital sovereignty and strategic autonomy, many of the EU's digital and cybersecurity policies are in a process of geopoliticisation. For example, Von der Leyen (2019) unapologetically positioned her Commission as 'the geopolitical Commission (…) that Europe urgently needs'. Whereas we have often seen politicisation of policies – in the sense of policies serving other purposes than the formal primary focus, for example, in trade – the backdrop of cyberspace and digital technologies as rather uncharted and contested territories for strategic competition steers relevant policies firmly in a geopolitical direction.

Given the challenges, the EU is looking to chart a course between protecting the internal market without overstepping the line of protectionism. But the EU will also need to invest in new technologies and markets, facilitate and organise intra-EU cooperation and build supporting (legal) frameworks. Overall, the challenge for the EU is to assert itself as a geostrategic power, without undercutting its already contested (self-) image of being a regulatory and normative power. However, given the limited competence of the EU in foreign affairs, and fiercely protected member state prerogatives when it comes to (national) security, unity and resolve are often lacking at the EU level. The strength of the EU as an international actor is greatly influenced by the legal basis of the policies it enacts. Policies pertaining to the internal market, covered by established rules and institutions and sometimes described as 'pooled' or 'delegated' sovereignty (Moravcsik 1998, p. 67), enable the EU to act more like a unitary actor commanding the weight of the internal market and its regulatory power in the international domain. The so-called Brussels effect is mostly linked to this domain (Bradford 2020). In the geopolitical domain, the EU has traditionally had less clout. Former Belgian foreign minister Eyskens once described Europe as 'an economic giant, a political dwarf, and a military worm' (cited in Manners 2010, p. 75). Whilst this may be an overly harsh judgement, the EU's lack of a clear competence in geostrategic matters makes it very hard for member states to agree on joint strategic positions.

This article analyses the EU's recent use of terminology on digital sovereignty and strategic autonomy to shed light on the contention between the EU's geopolitical ambitions and its traditional role as an economic and normative power. The emphasis is on recent policies and politics – sovereignty and autonomy have been coming up roughly

since 2016 in the context of the EU – but sometimes we consider earlier developments. We trace elements of this contention across relevant EU policies and politics on cybersecurity and digital technologies and their governance. The article does not aim to delineate a genealogy of an 'EU narrative' on digital sovereignty through formal and systematic discourse analysis but instead proposes to interpret elements of the use of this new terminology as indicators of the role of the EU as normative power vis-à-vis its geopolitical ambitions.

The article proceeds by situating digital sovereignty and strategic autonomy in the wider literature on sovereignty, focusing on the concepts of control and authority (Section II), and how the EU uses this terminology in relation to geo-economic and geo-political policy goals and the protection of free trade principles and fundamental rights (Section III). Section III analyses how notions of sovereignty and autonomy are slowly 'geopoliticising' the EU's digital policies, highlighting three policy trends: first, the instrumental use of 'classic' internal market policies; second, policies that aim to impose foreign policy 'requirements' on national markets; and third, a new generation of hybrid digital policies. The paper concludes that technological sovereignty inevitably entails policy trade-offs between internal market considerations, the EU's geopolitical position and the bloc's fundamental rights agenda. Moreover, for the EU as an actor, strategic autonomy is more likely in policies built on the community method, whilst strategic cacophony is more of a risk in the foreign policy domain.

I. Sovereignty between Authority and Control

In and through Cyberspace

Contemporary sovereignty is no longer conceived as an exclusive feature of statehood but also as a practice that unfolds through the exercise of different degrees of authority and control, with an internal and an external dimension. It was primarily in response to the European disastrous authoritarian experiences of 'the short twentieth century' (Hobsbawm 1995) that traditional state-centric conceptions of sovereignty were questioned through the introduction of legal and institutional 'limitations' and conditionalities to the sovereign countries' ability to exercise absolute control (Krasner 2004). Moreover, with the end of the Cold War, and the spread of neoliberalism across Europe, 'the market' increasingly acquired autonomy from national control, further diluting sovereign prerogatives to non-state actors (Jones 2003).

In *Sovereignty: Organised Hypocrisy* Krasner (1999, pp. 9–25) famously captures the dynamic characteristics of contemporary sovereignty in a fourfold categorization: (1) international legal sovereignty; (2) Westphalian sovereignty; (3) domestic sovereignty; and lastly (4) interdependence sovereignty, meaning a government's capacity to control cross-border movements of any kind (ideas, goods, people). Importantly, Krasner (1999, p. 10) makes a distinction between *authority* and *control* as two different goals and approaches of how sovereignty is exercised: 'authority involves a mutually recognized right for an actor to engage in specific kinds of activities (…) control can be achieved simply through the use of brute force with no mutual recognition of authority at all'. Ideally, states want authority and control to be coterminous, not in the least because a prolonged loss of control may undermine the formal/legal authority that underpins

sovereignty. This broader and dynamic understanding of sovereignty offers important insights for understanding how the concept has been used in relation to cyberspace and digital technologies.

The emergence of cyberspace initially contested the possibility of national/international territory and political authority but soon became a domain of fierce geopolitical competition (Healey 2013). The question of how to think of cyberspace as a domain of sovereignty sparked academic and policy debates that touch upon all four modes of Krasner's conceptualisation. Primarily, the question of sovereignty in cyberspace has been studied largely through a 'territorial ontology' (Cristiano 2019; Lambach 2020). International law scholarship has worked on the questions of if, how and when cyber operations constitute a violation of territorial sovereignty (Schmitt and Vihul 2017; Delerue 2020; Roguski 2020; Moynihan 2021). Another contested debate has been on whether it is possible and appropriate to reproduce the Westphalian system in cyberspace by fragmenting it into national segments (Demchak and Dombrowski 2013; Broeders 2015; Mueller 2017, 2020).

In addition to the idea of territorial cyberspace, scholarly thinking on sovereignty and cyberspace has also problematically turned to questions of how political authority and control are defined in relation to information, data and digital technologies more generally. Recent review articles analyse strategies of 'digital', 'technological' and 'data' sovereignty to make sense of these relatively new policy 'flags' (Baezner and Robin 2018; Couture and Toupin 2019; Hummel et al. 2021). Many of these policy strategies can be understood as seeking to reinforce what Krasner defined as interdependence sovereignty and are focused primarily on control, both internally and externally. The Russian and Chinese notions of digital sovereignty focus on the control of internal and external information flows (Broeders et al. 2019; Creemers 2020; Kurowska 2020). These interpretations of digital sovereignty are usually justified in terms of the people's right to self-determination and aim to block the interference of quasi-sovereign tech giants, foreign state intervention and the free flow of information, all of which are considered a threat to regime continuity. Worries about the power and state-like role of big tech companies have spread wide and underpin some of the European concerns when it comes to digital sovereignty. In recent years, the EU, whilst resisting the 'authoritarian model', has started to relate sovereignty to information flows and technology in cyberspace, seeking to increase control under the flag of digital or technological sovereignty. This new mission can be seen as the EU's way of repositioning itself as a security actor despite lacking control over more traditional security forces like the military and the police (Bellanova et al. 2022).

The EU: Pooled Sovereignty and 'Normative Power'

Like cyberspace, EU integration challenges the traditional understanding of sovereignty. The EU is a prime case for studying the transformation of sovereignty and its relation to economics and geopolitics. Together with the international conventions on human rights, EU integration is historically one of the most prominent curtailments of nation-state-centric sovereignty (Krasner 1995). As a result of this process, both the EU and its member states currently lack full-fledged sovereign prerogatives and the ability to exercise absolute control. Member countries retain many competencies, especially those

related to national defence and security, but most of them are not traditionally sovereign when it comes to, for instance, governing their currencies, common market policies and a number of technology-related policies, which they administer in cooperation with EU authorities on the basis of EU regulations and the EU treaties.

However, EU integration does not automatically imply that member countries have necessarily 'lost' their national sovereignty. Rather, it has been argued that the sovereignty of all EU states might be enhanced thanks to the EU cooperation and consultation system, as it makes them carry more political weight (Gourdault-Montagne and Ischinger 2008). This has been described as 'pooled sovereignty' (Peterson 1997; Moravcsik 1998). With sovereignty understood as a Krasnerian combination of control and authority in certain policy areas, the EU's 'pooled' or 'transferred' sovereignty is strongest – but not necessarily uncontested – in those policy areas where EU integration has gone farthest. The internal market – as the core of the EU treaties – has the deepest integration and the most established roles and responsibilities of the EU institutions. Here, authority and control are arguably most closely aligned at the level of the EU institutions, giving the EU political weight and some semblance of a sovereign actor in international relations. Sometimes, the loss of authority increases control, albeit at the EU level. The reverse is also possible: transferring authority can also lead to a decrease in control at the national level, for example, in the case of the internal Schengen borders. The core treaties of the Union seem the most solid ground available to build 'EU sovereignty' in the digital sphere. However, many of the 'threats' that the sovereignty and strategic autonomy debates are a reaction to are not (solely) economic issues but are closely linked to geopolitical posturing and strategic and national security issues. For example, the Common Foreign and Security Policy (CFSP) is a much less established policy area within the EU that is not covered by the community method of integration. Even though the EU aspires to become more of a security actor by means of the CFSP, joint positions are not a given as different member states have different foreign policy priorities, depending on history, geography and economic interests (Bradbury 2009).

Whilst lacking formal sovereign authority on geopolitical issues, the EU has traditionally asserted itself as a *normative power* (Manners 2002; Whitman 2011). Proponents of the EU as normative power, and the EU itself, have identified two means through which this power operates: first, the protection of fundamental rights at home and abroad and, second, the championing of free trade and technological progress. More specifically, the protection of fundamental rights 'is a founding principle of the Union and an indispensable prerequisite for its legitimacy' (von Bogdandy 2000, p. 1307). Market freedom has been a constant feature of the EU's strategic identity since the mid-1980s (Bicchi 2006; Scheipers and Sicurelli 2007). Since the successful Eastern integration in the 2000s, the EU became much more confident in its international role as promoting a rules-based system anchored in multilateral cooperation, good governance, rule of law, human rights and liberal democratic values (Michalski and Nilsson 2019, p. 434). Others have criticised the EU's self-portrayal as normative power in relation to its underlying and inherent politicisation and instrumental use (Hyde-Price 2006; Forsberg 2011).

II. Digital Sovereignty and Strategic Autonomy in EU Politics

The EU as a Normative Power on Cyberspace and Digital Technologies

Technological innovation and progress have played a crucial role in the process of European integration since its outset and have been deeply ingrained in the narrative of the EU as a normative power (Misa and Schot 2005). References to a 'European technological gap' – both internally between member states and externally vis-a-vis global powers – have accompanied the policy discourse on the Old Continent from the aftermath of World War II to the present day. As argued by Monsees and Lambach (2022, p. 380), it was, however, only with the emergence of the 'digital' as a specific policy domain that the EU 'levelled-up' its game and starkly referred to technological innovation as a geopolitical issue, besides being one of economic competitiveness.

With the emergence of the internet as a distinct policy domain, the two main normative strands of EU integration – liberal market values and the protection of human/individual rights – also came together. The traditional take of the EU and its member states on the internet envisions a technology that should be free, open, accessible and secure. The early internet freedom foreign policy agendas of the late 2000s – with the main emphasis on freedom and human rights – were already supplemented with a more economic agenda (DeNardis 2014; Broeders 2015). Now geopolitical and economic strife has put the EU on the path of finding a *third way* between the United States and China, putting further pressure on its normative agenda. Trade policies were always 'the core instrument of the EU's civilian power and, therefore, its political influence on the rest of the world' (Meunier and Nicolaidis 2019, p. 105). Whereas earlier the EU used its commercial power to promote its values in other parts of the world, recent trade deals harness that power to strategic ends instead (Meunier and Nicolaidis 2019). In digital policies, the existence of both competitor states and global technology companies and platforms has raised the bar even further in terms of reconciling economic competitiveness, technological (in)dependence and safeguarding fundamental rights.

The EU's normative power ambition, based on the protection of both human rights and market freedom, may be at odds with the new frame of cyberspace and emerging digital technologies as both a threat and an asset to the Union's strategic agenda. At the same time, technological progress represents a central item of the EU's normative role both internally and internationally, with issues such as technological cohesiveness and technological transfer high on the EU policy agenda (European Commission n.d.; Monsees and Lambach 2022). At a general level, the EU's economic interests are of course far wider than the bloc's normative, economic agenda of stimulating free trade principles. In parallel to digital or technological sovereignty, the EU started to use the terminology of strategic autonomy, which originated in the national security and military domain, or, more specifically, the development of an autonomous EU defence capacity (Meijer and Brooks 2021, p. 7). Even though strategic autonomy in the digital realm is not a military affair, the strategic security component makes it vulnerable to the fact that EU member states jealously guard foreign policy as a national prerogative and that the perceptions of threat vary wildly amongst member states (Faupin and Karkoszka 2003; Rynning 2003). Moreover, the use of more assertive and openly strategic terminology may undermine some of the EU's normative agenda and risk resonating with authoritarian

cyber sovereignty narratives of control of (national) cyberspace (Pohle 2020; Broeders et al. 2021). We will return to this point in Section III when we discuss specific policies.

The EU as a Digital Sovereign: Terminology

There are several concepts that the EU and its member states use when referring to digital sovereignty concerns, including strategic autonomy, technological sovereignty and data sovereignty. The EU Commission mostly refers to strategic autonomy and technological sovereignty. Both concepts emerged prominently in the EU's 'Global Strategy for Foreign and Security Policy' (EU External Action Service 2016). In deciding how to implement the Global Strategy, the Council defined strategic autonomy as the 'capacity to act autonomously when and where necessary and with partners wherever possible' (Council of the European Union 2016, p. 2). Questions about his somewhat vague definition led Josep Borrell, the EU's top diplomat, to author a lengthy blog post reaffirming that strategic autonomy was meant to help Europeans 'take charge of themselves' in an 'increasingly harsh world' and explaining why the concept should be understood as going beyond security issues to encompass also finance and investment (Borell 2020). As an example of an effort to bolster European strategic autonomy, Borrell pointed to the launch of the European Raw Materials Alliance (ERMA) in 2020, which helps companies and government secure access to critical materials such as rare earth elements, crucial for technology manufacturing. Such efforts to reduce dependency on external providers and manufacturers and secure technology supply chains have meant that the concept of strategic autonomy has also percolated into the digital debate (Pohle 2020, p. 12; Farrand and Carrapico 2022; Soare forthcoming).

Other EU representatives have echoed similar sentiments; Charles Michel stated boldly that strategic autonomy meant the EU achieving '[l]ess dependence [and] more influence' as a 'world power' (Michel 2020). The increasing usage of the term can therefore be seen as a direct result of the EU claiming its position as a peer competitor to other great powers and securing its vital interests in a multipolar world (Grevi 2020, p. 1; Soare forthcoming).

The second key concept used by the EU is technological sovereignty, meaning 'the capability that Europe must have to make its own choices, based on its own values, respecting its own rules' specifically in relation to technology (von der Leyen 2020). The 2020 EU Cybersecurity Strategy regards technological sovereignty, alongside resilience and leadership, as part of its first priority 'area of action'. More specifically, to reduce foreign dependencies, it foresees a wide range of activities: building and securing critical infrastructure and services, creating an EU 'cyber shield' to monitor cyber intrusions in real time, securing satellite communications, building EU 5G infrastructure, regulating Internet of Things devices, ensuring the functionality of the DNS root system, bolstering the EU's role in the global technology supply chain and developing a skilled European workforce (European Commission 2020a, pp. 5–12). The growth in the popularity of this term at the EU level since 2016 has also been spurred by declining international cooperation and resurfacing geopolitical concerns. These pressures were especially visible in 2019 during the debate about the inclusion of China's Huawei in the building of European 5G infrastructure, which the United States fiercely

resisted (Burwell and Propp 2020, p. 3) but received different responses in different EU member states (Radu and Amon 2021).

By using the terms strategic autonomy and technological sovereignty, the EU is trying to position itself as a more self-assured third actor (Farrand and Carrapico 2022; Monsees and Lambach 2022). In announcing the EU's new trade strategy, intended to support its digital transformation, Trade Commissioner Valdis Dombrovskis cautioned that the EU was 'pursuing a course that is open, strategic and assertive, emphasising the EU's ability to make its own choices and shape the world around it …' (European Commission 2021a).

The term data sovereignty is more specific than the previous two concepts. It implies the EU having control over how the data of EU citizens is used and, in relation to industrial data, enabling Europe to become a leader in the data economy (European Commission, 2022).

The Gaia-X initiative, which involves the development of a European data infrastructure, is an example of a major project intended to strengthen the EU's data sovereignty (we will return to Gaia-X in Section III). This European concern about data protection is not new. The bloc has over time gained a reputation for its activist legislation in this area: it adopted the Data Protection Directive already in 1995 and the General Data Protection Regulation (GDPR) in 2016. In a testament to the EU's enormous regulatory influence, many third countries subsequently introduced similar data protection rules in their own legislation to retain access to EU markets (Yakovleva and Irion 2020, p. 215). Whilst data privacy is often correctly considered to be part of the EU's fundamental rights agenda, the concept of data sovereignty has also gained a geopolitical angle. Its strategic motivations are particularly visible in the increasingly loud voices advocating for data localisation – the storage and processing of EU data in servers located within member states (Christakis 2020, p. ii). In no uncertain terms, Thierry Breton, the EU Internal Market Commissioner, explained that:

> it is necessary to structure the information space, as we have organised in the past the territorial space, the maritime space, and the airspace. The GAFA [Google, Amazon, Facebook, and Apple] tried to make a digital 'no man's land' whose laws they would write. It's over. It's time to relocate this information space by opting for processing our data on European soil. (Breton in Claypoole 2021)

As Breton's remarks indicate, much of the EU's motivation for regulating data is derived from a desire to reign in large technology platforms whose increasing power is believed to have given rise to a new era of 'surveillance capitalism' (Zuboff 2019). Whilst the United States believes in market-based regulation of technology companies, the EU wishes to enact more stringent, values-based regulation principles for online platforms (Schaake in: European Council on Foreign Relations 2020; Baker-Beall and Mott 2022) asserting a right to protect its citizens transnationally.

These pronouncements, however, sit awkwardly alongside the EU's calls for the free flow of data for fostering digital innovation, which has to date been sluggish in Europe (Burwell and Propp 2020, p. 5; Christakis 2020, p. 98). They have also opened up the EU to charges of discriminatory regulation and even Chinese-style protectionism (Christakis 2020, pp. 98–99). Charlene Barshefsky, a former US trade representative, wrote that the EU's 'discriminatory digital services taxes', 'rigged competition laws' and 'unjustified barriers for foreign AI applications', which are all part of the EU's digital

sovereignty agenda, mean that 'US policymakers will have no choice but to treat it as a strategic threat' (Barshefsky 2020).

In spite of EU denial of charges of protectionism (Merkel et al. 2021), the key concepts falling under the wider category of digital sovereignty indicate a decisive shift in EU thinking from its traditional defence of multilateralism towards clear expressions of self-interest and geopolitical positioning vis-à-vis China and the United States in the areas of technology, trade and investment (Farrand and Carrapico 2022). Spurred by the 'fundamentally asymmetrical nature of [economic] interdependence' and concerns that 'the weight of Europe in the world is shrinking', EU policymakers are resolute in securing what they see as the bloc's 'political survival', even if these actions jar with the EU's championing of free trade and risk irritating traditional allies (Borell 2020). In the following section, we will explore in more detail how the expression of geopolitical motivations in technology-related policies may create tensions with the EU's free market principles.

III. The Geopoliticisation of EU Digital Policies

The EU's geopolitical posturing by stressing its digital sovereignty and strategic autonomy has given rise to a number of new policy initiatives, as well as change in the implementation of existing policy. We note two broad policy considerations. Firstly, policies may be aimed at competitor or even adversarial countries (like the United States and China), at large technology companies, or at both (GAFA and the United States, Huawei and China). The EU's authority and control over its digital future requires limitations to both foreign commercial and foreign state power. Conversely, policies may also be aimed at building up joint EU capacity and resources. However, this often also requires shielding the EU off from foreign competitors. Secondly, the EU can geopoliticise existing policies and *regimes* – mostly established common market policies – or it can draft new policies to serve its geopolitical needs.

In our analysis, we discern three developments in EU policy-making and implementation that together point to a geopoliticisation of EU digital policies. These are, firstly, the instrumental use of 'classic' internal market policies, such as trade and competition policy, to exert geopolitical influence; secondly, policies that aim to impose foreign policy 'requirements' and restrictions on national markets, such as the 5G toolbox; and thirdly, a new generation of intentionally hybrid digital policies in which internal market concerns, fundamental rights and geopolitical concerns are all present, such as the AI-Act and the DSA/DMA. Given the Commission's strong competence in the internal market and the relatively limited competence in common foreign and security policy, the EU is likely to have more geo-economic and geo-political clout in internal market and hybrid policies. These policy choices will interact with the EU's (self-constructed) identity as a normative power as market protection may border on protectionism and geostrategic choices may come at the expense of the EU agenda of championing free trade and fundamental rights.

Instrumental Use of Internal Market Policies

EU competition law, trade and data protection law are examples of the instrumentalisation of internal market policies for geopolitical signalling. For example, EU competition law, in particular the prohibition of the abuse of a dominant position (Article 102, TFEU), has

been used to fine Microsoft, Intel and Google (Ibáñez Colomo 2018; Szczepański 2019). Currently, Amazon and Apple are also under investigation for abusing their dominant market position (European Commission 2019, 2020c). Given the wide range of possible cases, it is no coincidence that the EC chose so many big tech-related cases. These cases can be seen both as 'regular' competition law cases as well the EU signalling to American companies and the US government. However, the well-established procedures make it hard to instrumentalise competition policy much beyond the selection of cases (Monti 2022).

The EU's General Data Protection Regulation (GDPR) and the Data Protection Directive before it constitute another example of how market policies have become embedded in the terminology of digital sovereignty. Under the terms of the GDPR and regardless of where they are located or conduct business, organisations are required to abide by very strict data management rules when dealing with EU customers and users. The GDPR is part of a broader and very stringent data protection framework that, with the stated ambition of empowering EU citizens with more control over their data, instrumentalises the EU's acclaimed normative power on data protection issues to extend control on the internal market. As the GDPR prescribes substantial financial sanctions, it can be argued that the EU has imposed a stricter control on its internal market. For example, the Luxembourg DPA recently fined Amazon for the amount of $888 million. Fines are in a sense akin to sanctions, an instrument commonly employed in the context of foreign policy to address sovereign entities or their proxies. In addition to this internal market dimension, the EU's normative role on data protection matters also entails an external dimension, as the Union has also promoted a strategy for international data protection standards (Bradford 2020). The external effect of the EU data protection regulations is also visible in the two landmark EU Court cases of Schrems I and Schrems II, which rendered the data exchange arrangement between the EU and the United States – firstly the 'EU-US Safe Harbour agreement' and secondly the 'Privacy Shield' – invalid, amongst others for reasons of inadequate protection of EU data against American law enforcement and intelligence agencies. Although this was not the Commission speaking, the EU institutions did send a clear signal about surveillance to the United States in the wake of the Snowden revelations.

A different example of an internal market policy with a geopolitical aspect is Gaia-X, a project to build a 'federated, open data infrastructure based on European values' (GAIA-X n.d.) founded by 22 German and French organisations and companies (Cerulus 2020; Moerel and Timmers 2021, p. 8). The initiative is based deliberately on the principles of 'sovereignty by design' (Cerulus 2020; Moerel and Timmers 2021, p. 6). It was launched after Germany and France resolved that the EU was transferring too much valuable data away from its automotive, healthcare and finance sectors to US cloud providers (Green 2021). According to German Economy Minister Peter Altmaier, Gaia-X 'enables digital sovereignty for cloud service users' because 'European providers of cloud services can scale their uses so that it is economically attractive to offer these services' (Altmaier cited in: Noyan, 2021). By setting standards for easier data sharing between different European cloud providers, the designers of Gaia-X hope to reduce Europe's dependence on American technology giants by increasing the competitiveness of European companies (a geopolitical move) and, keeping in line with the mission to protect fundamental rights, enhance customers' control over who stores their data and

how it is processed (Moerel and Timmers 2021, p. 6). Additionally, it aims to increase the EU's control over the future value that developments in technology, such as edge computing, will generate (Timmers 2021). Although Gaia-X is open to American companies, in principle, it requires all of its participants to subscribe to a set of rules and technical requirements, including European data protection legislation and rules on the individual user's complete control over stored data.

Notably, however, at the time of writing, the project seemed to be in dire straits because of infighting and lack of cooperation between stakeholders. Moreover, major US cloud providers such as Microsoft are heavily involved in the development of the project and decisions on how to facilitate users' shifting their data to different providers, raising questions as to whether the project is still working mainly in European interests (Goujard and Cerulus 2021). The recent trajectory that Gaia-X has taken might in fact be undermining, rather than strengthening, its original goal of bolstering European strategic autonomy. However, the EU is starting to restrict international access to industrial alliances and is no longer as 'open to the world' as it used to be (Timmers 2022b). State aid regulations for Important Projects of Common European Interest point in a similar direction.

Imposing Foreign Policy 'Requirements' on National Markets

Secondly, we see a trend of imposing EU 'requirements' on national markets in light of foreign policy goals. The 5G toolbox and foreign direct investment (FDI) screening are examples of this development. In 2016, the EU developed a strategy 'to ensure Europe's leadership in 5G' and support the creation of a European 'home market' for 5G technologies (European Commission 2016). Recognising that the cybersecurity of 5G infrastructures is of 'strategic importance' due to the dependence of numerous critical services on their functioning, and in light of ever-increasing cyber-attacks from 'non-EU state or state-backed actors', the Commission has articulated concerns about increased exposure and vulnerabilities introduced by the roll-out of 5G, including the potential for supply chain attacks (European Commission 2020b, p. 4). The 2020 EU toolbox explicitly recognises that the cyber security of 5G networks is 'crucial for ensuring the technological sovereignty of the Union'. It introduces measures to mitigate the risks introduced by 5G networks and recommends that member states 'apply relevant restrictions for suppliers considered to be high risk' and 'necessary exclusions' for 'key assets' such as core network functions. They should also avoid dependency on a single supplier, particularly suppliers considered high risk (NIS Cooperation Group 2020). In a clear reference to China and Huawei, the Toolbox stipulates that the likelihood of interference from another state via a supply chain attack increases when there is, amongst other factors, '[a] strong link between the supplier and a government of a given third country', when 'there are no legislative or democratic checks and balances in place', or when a third country has the ability to 'exercise any form of pressure, including in relation to the place of manufacturing of the equipment' (NIS Cooperation Group 2020). However, in seeking to protect 5G networks, the EU has found it difficult to reconcile security with the principles of free trade (Dragne and Dragne 2020).

The recent EU framework for screening of FDI and state aid regulation for Important Projects of Common European Interest represent another example of how foreign policy

requirements are imposed on national markets. Operational since October 2020, the FDI has been presented as a direct conditionality (control) on the open market, grounded in the ambition of furthering EU integration (internal dimension) as well as a way to promote national responses to international security threats and vulnerabilities. Trade Commissioner Valdis Dombrovskis argued that the openness of the EU to FDI is not unconditional and the EU and the member states need to work closely together to safeguard their interest: 'If we want to achieve an open strategic autonomy, having an efficient EU-wide investment screening cooperation is essential' (European Commission 2020d). However, as the FDI screening regulation 'merely' provides a framework for member states, we can expect to see differences in the way individual member states deal with foreign investments.

'Hybrid' Digital Policies

A third development is the creation of new 'hybrid' policies, combining internal market, fundamental rights and geopolitical motivations, primarily in relation to emerging technologies. The proposed AI-Act is an example as it aims to improve the functioning of the internal market, address broad fundamental rights concerns (Veale and Zuiderveen Borgesius 2021, p. 3) and also send a geopolitical signal to foreign technology companies (so-called big tech) and their governments. It seeks to do this by regulating the entry of artificial intelligence (AI) systems to the EU market though a risk-based approach, identifying four levels of risk and banning 'unacceptable risk' systems because they would be in violation of fundamental rights. This proposed regulation of AI technologies, however, is the very opposite of the approach favoured by the United States, which prioritises AI innovation, voluntary standards and guidelines, and the application of existing consumer protection standards to new technologies (Meyers 2021). The EU's determination to pursue a divergent agenda with AI prompted Eric Schmidt, the Chair of the US National Security Commission on AI and former CEO of Google, to rebuke the EU for not seeking to become an 'innovation partner to the U.S.' (Haek 2021).

The Digital Services Act (DSA) and the Digital Markets Act (DMA) are two further examples of hybrid policy proposals. The stated objectives of the two policies are, first, 'to create a safer digital space in which the fundamental rights of all users of digital services are protected' and, second, 'to establish a level playing field to foster innovation, growth, and competitiveness' (European Commission 2021b). The first objective, through the DSA, seeks to address the issue of illegal exchange of goods online and the challenge of disinformation on social media platforms (European Commission 2021b). The second, embodied in the DMA, is a response to the 'gatekeeper' role of large platforms in digital markets, which, according to the European Commission, allows them to create unfair rules and restrict competition from smaller providers of similar services (European Commission 2021b). The DMA will consequently place 'ex-ante' obligations on platforms to address these 'egregious practices' (Breton 2021a). Whilst EU officials insist that the overarching aim of the policies is the '[e]mpowerment of citizens [and] of companies' in order to create a 'society of equals' (Viola in: IIEA 2021), in imposing controls on large American digital platforms, the larger effect of these two policies will be once again to send a geopolitical signal to the United States. In other words, when placed in the context of strategic autonomy and

digital sovereignty, both the DSA and DMA have become part of the EU's mission to demonstrate its more assertive position on the global stage. Or as Roberts et al. (2021, p. 14) phrase it, DSA and DMA are 'the creation of a regulatory framework that allows the EU authorities to pinpoint and sanction technology companies for a range of controversial practices that fly in the face of EU interests'.

Similar geopolitical undertones can be detected in the EU's announcement of an EU Chips Act. In 2021, Commission President Von der Leyen presented a proposal for an EU Chips Act as a new initiative that is 'not just a matter of our competitiveness' but 'also a matter of tech sovereignty'. In light of growing international semiconductor shortages, the global tech race and the recently enacted US Chip Act, Commissioner Breton (2021b) underlined the need for 'a coherent European vision and strategy' that is able to integrate national strategies to develop on their soil industrial and production capacities in order to reduce their dependencies efforts. He underscored that Von der Leyen's announcement was meant to send 'a strong geopolitical and economic signal'. However, strategic autonomy does not equal autarky as the EU cannot hope to become self-sufficient in terms of semiconductors. It will need strategic partners, like the United States, and will also need to avoid a counterproductive zero sum subsidy race (Timmers 2022a; Csernatoni 2022).

Conclusion

The use of digital sovereignty and strategic autonomy terminology create tensions with the EU's objective of being a normative power – an international position based on values and regulation – as it tries to take on a new role as a digital (geo)strategic power. An additional problem with what is still largely a shift in *political terminology* is that the EU is not well placed institutionally to become a geostrategic power as it lacks the mandate to do so and is reputationally bound to its fundamental values and open and free markets. These tensions can be detected in the policies themselves as EU thinking on digital sovereignty and strategic autonomy increasingly percolate into them. Established single market regimes like EU competition law have taken on many cases related to big American tech companies, pushing back against their influence and informally signalling the EU's position. More overt foreign policies targeting certain countries and their tech champions, like the EU foreign investment screening mechanism and the 5G toolbox, are now becoming part of the assessment framework for how the digital market(s) in Europe should develop. And more recent policy proposals like the AI-Act, the Chips Act and the DSA and DMA acts are more openly a mix of market and consumer protection on the one hand and a rebuff of foreign influence in the EU (markets) on the other. Sometimes, there is a productive overlap between different policy goals – protecting fundamental rights and signalling a more assertive EU position in data protection and digital markets, for example. Sometimes, there is more tension between economic and geostrategic goals on the one hand and the normative narrative of free trade on the other, for example, in potentially exclusionary and protectionist policies and investments such as 5G, FDI and the Chips Act. Also, using EU market access as leverage to support the EU's fundamental rights agenda elsewhere in the world, often used in trade and other policies, may increasingly give way to the demands of a more narrowly interest-based strategy of digital sovereignty and strategic autonomy.

Although the EU is a formidable actor when it comes to the internal market and internal market regulation – evidenced by the so-called Brussels effect – it has a limited (and shared) mandate and capabilities when it comes to foreign policy and defence. Whilst the context of cyberspace increasingly requires strategic, geopolitical thinking and action, the EU is institutionally not well equipped to deliver on a strategy of strategic autonomy. Member states' individual foreign policies and national interests pose a formidable obstacle to a unified security strategy. Of the three main policy developments described in this paper – instrumental use of 'classic' internal market policies; policies that aim to impose foreign policy 'requirements' on national markets; and the new generation of hybrid digital policies – the second one is especially vulnerable. These developments may entail two risks for the EU. Firstly, there is a danger that front lining a geopolitical strategy in the digital realm will lead to 'strategic cacophony', meaning large divergences across member states' policies (Meijer and Brooks 2021), rather than the strategic autonomy, however ill-defined, that the EU seeks. We are already witnessing this cacophony to a certain extent with the differing approaches of member states to the protection of 5G supply chains, as well as with the recent developments in Gaia-X. Secondly, geopolitical posturing and the unabashed defence of interest-driven behaviour are likely to harm the potential diffusion of the EU's normative leadership. Since the 1980s, the EU has carefully crafted its international image as a role model of foreign policy decision-making based on liberal values and free market principles. In the digital realm this role was translated into the defence of a free, open, accessible and secure internet that has underpinned European diplomatic and capacity building efforts internationally. Digital sovereignty and strategic autonomy, and the market restrictions that they entail, do not comfortably align with these principles and have even prompted charges of protectionism.

Acknowledgements

This study was conducted as part of the work of The Hague Program on International Cyber Security, which is funded by the Dutch Ministry of Foreign Affairs. Earlier versions were presented at the 2021 conference Governing Through Crisis: Conflict, Crises and the Politics of Cyberspace in The Hague and the 2022 conference European Governance of Emerging Technologies: Concepts, Challenges and Practices in Paris. The authors wish to thank Jonathan Arendsen for his research assistance and Els de Busser, François Delerue and Raluca Csernatoni and two anonymous reviewers for their comments on earlier versions.

Correspondence:
Dennis Broeders, Institute of Security and Global Affairs (ISGA), Leiden University, PO Box 13228, 2501 EE The Hague, The Netherlands.
email: d.w.jbroeders@fgga.leidenuniv.nl

References

Baezner, M. and Robin, P. (2018) *Cyber Sovereignty and Data Sovereignty. Version 2, Cyberdefense Trend Analysis* (ETH Zürich: Center for Security Studies (CSS)).

Baker-Beall, C. and Mott, G. (2022) 'Understanding the European Union's Perception of the Threat of Cyberterrorism: A Discursive Analysis'. *JCMS: Journal of Common Market Studies*, Vol. 60, No. 4, pp. 1086–1105.

Barrinha, A. and Christou, G. (2022) 'Speaking sovereignty: the EU in the cyber domain'. *European Security*, Vol. 31, No. 3, pp. 356–376. https://doi.org/10.1080/09662839.2022.2102895

Barlow, J. (1996) *A Declaration of Independence of Cyberspace* (Electronic Frontier Foundation).

Barshefsky, C. (2020) EU digital protectionism risks damaging ties with the US. *Financial Times*. https://www.ft.com/content/9edea4f5-5f34-4e17-89cd-f9b9ba698103

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

Bicchi, F. (2006) ''Our Size Fits All': Normative Power Europe and the Mediterranean'. *Journal of European Public Policy*, Vol. 13, No. 2, pp. 286–303.

Borell, J. (2020) 'Why European Strategic Autonomy Matters'. EU External Action Service (EU EEAS). https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en

Bradbury, J. (2009) 'The European Union and the Contested Politics of 'Ever Closer Union': Approaches to Integration, State Interests and Treaty Reform since Maastricht'. *Perspectives on European Politics and Society*, Vol. 10, No. 1, pp. 17–33. https://doi.org/10.1080/15705850802699961

Bradford, A. (2020) *The Brussels Effect. How the European Union Rules the World* (Oxford: Oxford University Press).

Breton, T. (2021a) DSA/DMA myths – Will the EU regulation favour single-service companies? LinkedIn. https://www.linkedin.com/pulse/dsadma-myths-eu-regulation-favour-single-service-companies-breton/?trk=read_related_article-card_title

Breton, T. (2021b) How a European Chips Act will put Europe back in the tech race. https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-chips-act-will-put-europe-back-tech-race_en

Broeders, D. (2015) *The public core of the internet: An international agenda for internet governance* (Amsterdam: Amsterdam University Press).

Broeders, D. (2022 'Digital Sovereignty: From Narrative To Policy? EU Cyber Direct'. https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Broeders, D., Adamson, L. and Creemers, R. (2019) 'Coalition of the unwilling? Chinese and Russian perspectives on cyberspace'. The Hague Program For Cyber Norms Policy Brief. November 2019.

Broeders, D., Cristiano, F. and Weggemans, D. (2021) 'Too close for comfort: cyber terrorism and information security across national policies and international diplomacy'. *Studies in Conflict & Terrorism*, pp. 1–28. https://doi.org/10.1080/1057610X.2021.1928887

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

Burwell, F. and Propp, K. (2020) The European Union and the search for digital sovereignty: Building 'Fortress Europe' or preparing for a new world? Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/the-european-union-and-the-search-for-digital-sovereignty/

Cerulus, L. (2020) Europe's litmus test over cloud computing push. Politico. https://www.politico.eu/article/shades-of-sovereignty-dent-european-cloud-dreams/

Christakis, T. (2020) 'European digital sovereignty': Successfully navigating between the 'Brussels effect' and Europe's quest for strategic autonomy. Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute. https://doi.org/10.2139/ssrn.3748098

Claypoole, T. (2021) Data localization and the limits of "everything from everywhere". Lexology. https://www.lexology.com/library/detail.aspx?g=f6d4446d-342f-4d07-9253-d108f0104909

Council of the European Union. (2016) Council conclusions on implementing the EU global strategy in the area of security and defence. https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.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.

Creemers, R. (2020) 'China's Conception of Cyber Sovereignty: Rhetoric and Realization'. In Broeders, D. and van den Berg, B. (eds) *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield).

Cristiano, F. (2019) 'Deterritorializing Cyber Security and Warfare in Palestine: Hackers, sovereignty, and the National Cyberspace as Normative'. *CyberOrient*, Vol. 13, No. 1, pp. 28–42.

Csernatoni, R. (2022) 'The EU's Chips Act: A new piece in the digital sovereignty puzzle'. In Broeders, D. (ed.) *Digital Sovereignty: From Narrative To Policy? EU Cyber Direct*. https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Delerue, F. (2020) *Cyber Operations and International Law* (Cambridge (UK): Cambridge University Press).

Demchak, C. and Dombrowski, P. (2013) 'Cyber Westphalia: asserting state prerogatives in cyberspace'. *Georgetown Journal of International Affairs*, Vol., No. Special Issue, pp. 29–38.

DeNardis, L. (2014) *The Global War for Internet Governance* (New Haven and London: Yale University Press).

Dragne, I. and Dragne, A. (2020) Compatibility of 5G cyber security measures with free trade. The Legal 500. https://www.legal500.com/developments/press-releases/compatibility-of-5g-cyber-security-measures-with-free-trade/

EU External Action Service. (2016) 'Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy'. https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

European Commission. (2016) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 5G for Europe: An Action Plan. https://digital-strategy.ec.europa.eu/en/policies/5g-action-plan

European Commission. (2019) Antitrust: EC opens formal investigation against Amazon. https://ec.europa.eu/commission/presscorner/detail/en/ip_19_4291

European Commission. (2020a) The EU's cybersecurity strategy for the digital decade. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

European Commission. (2020b) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G deployment in the EU: Implementing the EU toolbox. https://digital-strategy.ec.europa.eu/en/library/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

European Commission. (2020c) Antitrust: Commission opens investigations into Apple. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1073

European Commission. (2020d) EU foreign investment screening mechanism becomes fully operational. Press release. 9 October 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1867

European Commission. (2021a) Commission sets course for an open, sustainable and assertive EU trade policy. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_644

European Commission. (2021b) The Digital Services Act package. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

European Commission. (2022) 'A European Strategy for Data'. https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission. (n.d.) Cohesion policy making Europe fit for the digital age. Retrieved 30 September 2022, from. https://ec.europa.eu/regional_policy/en/policy/how/priorities/digital-ag

European Council on Foreign Relations. (2020) Podcast: Conquering the cyber sphere: How the EU can build digital sovereignty. European Council on Foreign Relations. https://ecfr.eu/podcasts/episode/conquering_the_cyber_sphere_how_the_eu_can_build_digital_sovereignty/
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
Faupin, A. and Karkoszka, A. (2003) 'For a European Conference on Threat Perception'. *European Security*, Vol. 12, No. 2, pp. 117–121. https://doi.org/10.1080/09662830412331308136
Floridi, L. (2020) 'The Fight for Digital Sovereignty: What It IS, and Why It Matters, Especially for the EU'. *Philosophy & Technology*, Vol. 33, No. 3, pp. 369–378.
Forsberg, T. (2011) 'Normative Power Europe, Once Again: A Conceptual Analysis of an Ideal Type'. *JCMS: Journal of Common Market Studies*, Vol. 49, No. 6, pp. 1183–1204.
GAIA-X. (n.d.) GAIA-X: A federated data infrastructure for Europe. Data-Infrastructure.Eu. Retrieved 23 July 2021, from. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
Goujard, C. and L. Cerulus, (2021) Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project. Politico. https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/
Gourdault-Montagne, M. and Ischinger, W. (2008) 'Unity and Sovereignty'. The Guardian. https://www.theguardian.com/commentisfree/2008/jan/22/politics.eu
Green, A. (2021) Europe's Gaia-X looks to challenge big tech's cloud dominance. Financial Times. https://www.ft.com/content/6ac505fd-5b90-4979-8c3c-b5ba756e9089
Grevi, G. (2020) Fostering Europe's strategic autonomy: A question of purpose and action. European Policy Center and Konrad Adenauer Stiftung. https://www.epc.eu/content/PDF/2020/Final_Paper_Purpose_and_Action_Layout_JF_II__1_.pdf
Haek, P. (2021) Ex-Google boss slams transparency rules in Europe's AI bill. Politico. https://www.politico.eu/article/ex-google-boss-eu-risks-setback-by-demanding-transparent-ai/
Healey, J. (ed.) (2013) *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Vienna (Va.): Cyber Conflict Studies Association).
Herzog, D. (2020) *Sovereignty, RIP* (New Haven: Yale University Press).
Hobsbawm, E.J. (1995) *Age of Extremes: The Short Twentieth Century, 1914–1991* (London: Abacus).
Hummel, P., Braun, M., Tretter, M. and Dabrock, P. (2021) 'Data Sovereignty: A Review'. *Big Data & Society*, Vol. 8, No. 1, 2053951720982012.
Hyde-Price, A. (2006) ''Normative' Power Europe: A Realist Critique'. *Journal of European Public Policy*, Vol. 13, No. 2, pp. 217–234.
Ibáñez Colomo, P. (2018) 'The Future of Article 102 TFEU after Intel'. *Journal of European Competition Law & Practice*, Vol. 9, No. 5, pp. 293–303.
IIEA. (2021) Roberto Viola—Towards European digital sovereignty. Soundcloud. https://soundcloud.com/iiea/roberto-viola-towards-european-digital-sovereignty
Jones, E. (2003) 'Liberalized Capital Markets, State Autonomy, and European Monetary Union'. *European Journal of Political Research*, Vol. 42, No. 2, pp. 197–222. https://doi.org/10.1111/1475-6765.00080
Kello, L. (2017) *The Virtual Weapon and International Order* (New Haven and London: Yale University Press).
Krasner, S.D. (1995) 'Compromising Westphalia'. *International Security*, Vol. 20, No. 3, pp. 115–151.
Krasner, S.D. (1999) *Sovereignty: Organized Hypocrisy* (Princeton: Princeton University Press).
Krasner, S.D. (2004) 'Sharing Sovereignty: New institutions for Collapsed and Failing States'. *International Security*, Vol. 29, No. 2, pp. 85–120.

Kurowska, X. (2020) 'What Does Russia Want in Cyber Diplomacy? A Primer'. In Broeders, D. and van den Berg, B. (eds) *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield).
Lambach, D. (2020) 'The Territorialization of Cyberspace'. *International Studies Review*, Vol. 22, No. 3, pp. 482–506.
Liebetrau, T. (2022) 'Cyber Conflict Short of War: A European Strategic Vacuum'. *European Security*, Vol. 31, pp. 497–516. https://doi.org/10.1080/09662839.2022.2031991
Manners, I. (2002) 'Normative Power Europe: A Contradiction in Terms?' *JCMS: Journal of Common Market Studies*, Vol. 40, No. 2, pp. 235–258. https://doi.org/10.1111/1468-5965.00353
Manners, I. (2010) 'Global Europa: Mythology of the European Union in World Politics'. *Journal of Common Market Studies*, Vol. 48, No. 1, pp. 67–87.
Meijer, H. and Brooks, S.G. (2021) 'Illusions of Autonomy: Why Europe Cannot Provide for Its Security If the United States Pulls Back'. *International Security*, Vol. 45, No. 4, pp. 7–43. https://doi.org/10.1162/isec_a_00405
Merkel, A., Frederiksen, M., Marin, S. and Kallas, K. (2021) Letter from Germany, Finland, Estonia and Denmark for the EU. Valtioneuvosto Statsrådet. https://valtioneuvosto.fi/documents/10616/56906592/DE%2BDK%2BFI%2BEE%2BLetter%2Bto%2Bthe%2BCOM%2BPresident%2Bon%2BDigital%2BSovereignty_final.pdf/36db4c7f-3de9-103a-d01a-9c8ccd703561/DE%2BDK%2BFI%2BEE%2BLetter%2Bto%2Bthe%2BCOM%2BPresident%2Bon%2BDigital%2BSovereignty_final.pdf?t%3D1614670944134
Meunier, S. and Nicolaidis, K. (2019) 'The Geopoliticization of European Trade and Investment Policy'. *Journal of Common Market Studies*, Vol. 57, No. S1, pp. 103–113.
Meyers, Z. (2021) Reality bytes: The limits of transatlantic digital co-operation. Centre for European Reform. https://www.cer.eu/insights/reality-bytes-limits-transatlantic-digital-co-operation
Michalski, A. and Nilsson, N. (2019) 'Resistant to Change? The EU as a Normative Power and Its Troubled Relations with Russia and China'. *Foreign Policy Analysis*, Vol. 15, No. 3, pp. 432–449. https://doi.org/10.1093/fpa/ory008
Michel, C. (2020) 'Strategic autonomy for Europe—The aim of our generation'—Speech by President Charles Michel to the Bruegel think tank. Council of the European Union. https://www.consilium.europa.eu/en/press/press-releases/2020/09/28/l-autonomie-strategique-europeenne-est-l-objectif-de-notre-generation-discours-du-president-charles-michel-au-groupe-de-reflexion-bruegel/
Misa, T.J. and Schot, J. (2005) 'Inventing Europe: Technology and the Hidden Integration of Europe. Introduction'. *History and Technology*, Vol. 21, pp. 1–19.
Moerel, L. and Timmers, P. (2021) Reflections on digital sovereignty. EU Cyber Direct. https://eucyberdirect.eu/wp-content/uploads/2021/01/rif_timmersmoerel-final-for-publication.pdf
Monsees, L. and Lambach, D. (2022) 'Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity'. *European Security*, Vol. 31, No. 3, pp. 377–394. https://doi.org/10.1080/09662839.2022.2101883
Monti, G. (2022) 'EU competition law and digital sovereignty'. In Broeders, D. (ed.) *Digital Sovereignty: From Narrative To Policy? EU Cyber Direct*. https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy
Moravcsik, A. (1998) *The Choice for Europe. Social Purpose and State Power from Messina to Maastricht* (Cornell: Cornell University Press).
Moynihan, H. (2021) 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace'. *Journal of Cyber Policy*, Vol. 6, No. 3, pp. 394–410.
Mueller, M. (2017) *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* (John Wiley & Sons).
Mueller, M.L. (2020) 'Against Sovereignty in Cyberspace'. *International Studies Review*, Vol. 22, No. 4, pp. 779–801.

NIS Cooperation Group. (2020) Cybersecurity of 5G networks—EU Toolbox of risk mitigating measures. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Noyan, O. (2021) 'EU Countries Keep Different Approaches to Huawei on 5G Rollout'. Euractiv. https://www.euractiv.com/section/digital/news/eu-countries-keep-different-approaches-to-huawei-on-5g-rollout/

Peterson, J. (1997) 'The European Union: Pooled Sovereignty, Divided Accountability'. *Political Studies*, Vol. 45, No. 3, pp. 559–578. https://doi.org/10.1111/1467-9248.00096

Pohle, J. (2020) Digital sovereignty. A new key concept of digital policy in Germany and Europe. Konrad-Adenauer-Stiftung. https://www.econstor.eu/bitstream/10419/228713/1/Full-text-report-Pohle-Digital-sovereignty.pdf

Radu, R. and Amon, C. (2021) 'The Governance of 5G Infrastructure: Between Path Dependency and Risk-Based Approaches'. *Journal of Cybersecurity*. https://doi.org/10.1093/cybsec/tyab017

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M. and Floridi, L. (2021) 'Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies'. *Internet Policy Review*, Vol. 10, No. 3. https://policyreview.info/articles/analysis/safeguarding-european-values-digital-sovereignty-analysis-statements-and-policies

Roguski, P. (2020) 'Violations of Territorial Sovereignty in Cyberspace—an Intrusion-based Approach'. In Broeders, D. and van den Berg, B. (eds) *Governing Cyberspace: Behaviour, Power and Diplomacy* (London: Rowman & Littlefield).

Rynning, S. (2003) 'The European Union: Towards a Strategic Culture?' *Security Dialogue*, Vol. 34, No. 4, pp. 479–496. https://doi.org/10.1177/0967010603344007

Scheipers, S. and Sicurelli, D. (2007) 'Normative Power Europe: A Credible Utopia?' *Journal of Common Market Studies*, Vol. 45, No. 2, pp. 435–457.

Schmitt, M. and Vihul, L. (2017) 'Respect for Sovereignty in Cyberspace'. *Texas Law Review.*, Vol. 95, 1639.

Soare, S.R. (forthcoming) ''Algorithmic power? The role of artificial intelligence in European strategic autonomy'. In Cristiano, F., Broeders, D., Delerue, F., Douzet, F. and Géry, A. (eds) *Artificial Intelligence and International Conflict in Cyberspace* (Abingdon: Routledge).

Szczepański, M. (2019) *EU Competition Policy: Key to a Fair Single Market* (EPRS-European Parliamentary Research Service).

Timmers, P. (2019) 'Challenged by "Digital Sovereignty"'. *Journal of Internet Law*, Vol. 23, No. 6, pp. 11–23.

Timmers, P. (2021) 'Debunking Strategic Autonomy'. Directions Blog. https://directionsblog.eu/debunking-strategic-autonomy

Timmers, P. (2022a) How Europe aims to achieve strategic autonomy for semiconductors. Brookings Institute, 22 August 2022.

Timmers, P. (2022b) 'Investment policy for digital sovereignty: From policy to action'. In Broeders, D. (ed.) *Digital Sovereignty: From Narrative To Policy? EU Cyber Direct*. https://eucyberdirect.eu/research/digital-sovereignty-narrative-policy

Veale, M. and Zuiderveen Borgesius, F. (2021) 'Demystifying the Draft EU Artificial Intelligence Act — Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach'. *Computer Law Review International*, Vol. 22, No. 4, pp. 97–112. https://doi.org/10.9785/cri-2021-220402

von Bogdandy, A. (2000) 'The European Union as a human rights organization? Human rights and the core of the European Union'. *Common Market Law Review*, Vol. 37, No. 6, pp. 1307–1338. https://doi.org/10.54648/315870

von der Leyen, U. (2019) Speech in the European Parliament plenary session. 27 November 2019. https://ec.europa.eu/info/sites/default/files/president-elect-speech-original_1.pdf

von der Leyen, U. (2020) Shaping Europe's digital future: Op-ed by Ursula von der Leyen, President of the European Commission. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260

Whitman, R. (ed.) (2011) *Normative Power Europe: Empirical and Theoretical Perspectives* (Springer).

Yakovleva, S. and Irion, K. (2020) 'Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade'. *International Data Privacy Law*, Vol. 10, No. 3, pp. 201–221. https://doi.org/10.1093/idpl/ipaa003

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (London: Profile Books).