WORKING PAPER

The discursive performance of EU digital sovereignty: three co-performances

Wanshu Cong

European University Institute

Max Weber Programme

The discursive performance of EU digital sovereignty: three co-performances

Wanshu Cong

MWP Working Paper 2021/07

Views expressed in this publication reflect the opinion of individual author(s) and not those of the European University Institute.

This publication is available in Open Access in Cadmus, the EUI Research Repository:

Abstract

Digital sovereignty is now being spoken about regularly at both the EU and member state levels. While the notion expresses the EU's intention to achieve greater strategic autonomy and reduce external dependency, it has been criticized by commentators for lacking conceptual clarity. This paper argues that precisely because of its conceptual ambiguity, digital sovereignty has become a rich terrain for discursive performances that constitute the EU's relationship with various actors. This paper examines three discursive co-performances: between the EU and its main international interlocutors, i.e., the US and China, where a certain degree of imitation can be discerned; between the EU and its member states, where both convergence and dissonance of political motivations can be identified; and between the EU and activists for individual digital rights who appropriate the EU's sovereignty discourse to make it compatible with the rights-centered approach to data governance. These three co-performances reveal various contradictions surrounding digital sovereignty in the European context: the tendency of imitation in the first may undermine rather than reinforce the EU's autonomy; in the second, below the superficial level of coordination, competing interests of EU member states further fragment the EU's strategy and approach; in the third, the strategy of appropriation leaves critical questions of authority and representation unanswered, which risks weakening individual digital rights.

Keywords
Digital sovereignty, the European Union, discourse analysis, co-performance.

Wanshu Cong
Max Weber Fellow, 2020–2021

Introduction

> *In terms of economic value alone, this is a market worth tens if not hundreds of billions of euros per year. At a time when Europe desperately needs growth, this is exactly where we should be looking to create new jobs and new opportunities. That's why I've called data the new oil. Because it's a fuel for innovation, powering and energising our economy. Unlike oil, of course, this well won't run dry: we've only just started tapping it.*
>
> Neelie Kroes[1] (2013)

> *It's like with access to gas – if we make our entire energy supply rely on a few nations in the world who get to control access, we're becoming politically dependent.*
>
> Benjamin Strasser[2] (Delcker 2019)

The two extracts above show how the commonplace metaphor "data is the new oil" has significantly changed its meaning and connotation. While the metaphor was initially used by businessmen and policymakers to project the economic potential of data and to promote a data-driven economy, it now alludes to real possibilities of geopolitical rebalancing and the restructuring of the global economic order, suggesting the key to obtaining the upper hand in this game-changing process is control over data.

If we take the metaphor seriously, the return of geopolitics should not be surprising. After all, resource extraction and access to natural resources have been a crucial part of global power politics since the time of colonisation. But still, in mainstream scholarship on internet governance, the introduction of geopolitical elements to the domains of internet and data governance and the explicit language of sovereignty are often perceived as problematic. In brief, states claiming their sacred sovereignty are often seen as the foe of the liberalised system of global governance, while those restraining themselves from talking about power and upholding liberal values are the system's heroic defenders. The EU has conventionally positioned itself in the latter camp. Against this political and ideological background, it is interesting to note that the language of sovereignty is now gaining in popularity in the EU. The term "digital sovereignty" is being spoken regularly at both the EU and member state levels. At first glance, this explicit sovereignty framing appears in striking contrast with the EU's traditional self-understanding as an antithesis of power politics, and it signals, as Josep Borrell puts it, Europe speaking the language of power (Weiler 2020). Given the particular international contexts in which discourses of digital sovereignty have emerged in Europe, speaking the language of power also indicates a more explicitly assertive geopolitical stance: to become a global player and a "superpower in its own right" (Hobbs 2020).

To non-EU audiences, the call of European politicians to assert European power and sovereignty can sound hypocritical for various reasons. Apart from its relationship with its neighbours and Russia, in which geopolitics looms large, the EU has exercised vast regulatory power globally through what Anu Bradford (2020) calls "the Brussels effect", criticized by many commentators as imperialist (Bradford 2020, 247-48). In short, there is a considerable degree of irony in European politicians' depiction that the EU has been weak or has "completely abandoned what used to be the 'grammar' of sovereignty" (*The Economist* 2019), and that it has to start relearning that grammar now. Nevertheless, it is perhaps precisely that hypocrisy which suggests that, for the EU, speaking the language of power and sovereignty is not without difficulties. Superficially, invoking sovereignty to play geopolitics may appear regrettable in the

---

1 Then Vice-President of the European Commission responsible for the Digital Agenda.

2 A member of the German parliament from the Free Democratic Party.

eyes of proponents of the liberal international (economic) order. In addition, despite the deep roots of nationalism in Europe, the whole project of European integration is commonly depicted as a liberal enterprise that rejects both power politics and the notion of state sovereignty as being absolute and undivided (Schutze 2014). As we will see, the EU's justification seems to be that it joins the game of geopolitics, not to defeat, but to defend liberal values. In this view, the language of sovereignty and the return to geopolitics are means to a greater end, oriented towards an enlightened global order and hence different from nationalism or narrow Europeanism: in short, the assertion of EU digital sovereignty is not really a departure but a detour (Warlouzet 2020).

To explain how the EU's stance on digital geopolitics is constructed and what it entails for the EU and global data governance, this paper provides a discourse analysis on the EU's digital sovereignty, examining statements made by politicians, policymakers and think tanks in the EU and its member states. By adopting discourse analysis, the paper approaches "digital sovereignty" not as an abstract concept that has certain essential meanings but as a particular use of language whose meaning is embedded in its social contexts. Drawing from J.L. Austin's speech act theory and Hannah Arendt's political theory, the analysis in this paper conceives the EU's discourses of digital sovereignty as performance, and the context of the utterance and the audience as, at least, as important as the literal content of the discourse. In brief, the paper pays attention more to what the discourse of "digital sovereignty" does than what the term purports. Focusing on the contexts and audiences of the performance, I argue that the EU's discursive performance of digital sovereignty is inevitably co-performance: the EU's discourse is simultaneously constituted by the ways the audiences receive, interpret and react to it.

I discuss three co-performances. First, at the international level, the EU's audience is other international actors who present existential threats to the EU. For this particular co-performance, a certain degree of imitation can be discerned between the EU and its international interlocutors, notably the US and China. The analysis will focus on the critical question of to what extent imitation would reduce Europe's dependencies or further undermine its autonomy. This outward-looking dimension of the digital sovereignty discourse has reflexive effects, forging European collective identification. Hence, the second co-performance is at the EU level, with the EU member states. The analysis will show that pronouncements of sovereignty by the EU and its member states largely converge, but dissonance in this co-performance already exists and is expected to continue appearing. In addition to these external and internal co-performances between different polities, there is a third co-performance where civil societies and activists for individual digital rights join to make the EU's sovereignty discourse compatible with the rights-centered approach to data governance. The analysis will look at the discursive strategies of rights advocates to reconcile or temper their skepticism over sovereignty.

The paper proceeds in the following steps. First, I introduce the analytical framework in which this paper approaches "digital sovereignty", that is, from the perspective of discursive performance. From this perspective, the context and content of a discourse are intricately related. The paper then moves to discuss the internal and external conditions commonly picked up in policy discussions that paved the way for the EU's discourse to emerge. This is followed by an examination of the three discursive co-performances of "digital sovereignty", showing how different relationships reconfigure this discourse, and how this discourse restructures these relationships through co-performances. The paper concludes with a reflection on the various contradictions and tensions exposed in the three co-performances and their likely consequences for the EU.

Analytical framework: discourse analysis and the performative dimension of discourse

This paper enquires into the EU's discourses of digital sovereignty. While expressing the desire to exercise power and control, increase autonomy and reduce dependency and vulnerabilities,[3] discussions about digital sovereignty at the EU tend either to enumerate its elements, or to (re)brand policy priorities and agendas, rather than define the term. The effect of "listing + (re)branding" is that "digital sovereignty" becomes a "projection surface for a wide variety of political demands" (Christakis 2020, i). And because this term seems to encompass many different things, commentators have pointed out its lack of conceptual clarity (Kundnani 2020; Burwell and Propp 2020, 15). However, given the intrinsic elasticity of "sovereignty",[4] deploring the lack of clear definition of "digital sovereignty" is not particularly useful.

This paper draws on Austinian speech act theory and conceives the lack of definitional clarity of the EU's digital sovereignty as a starting point from which rich discursive performances of various actors emerge. The diversity of actors and performances is nothing unusual, since neither the EU, as a regional bloc, nor its bodies, such as the European Commission, is homogenous. I approach the issue of the EU's digital sovereignty by examining those discursive performances and their consequences. Instead of seeing "digital sovereignty" as an abstract concept whose precise content and contour need clarification, I am interested in the ways "digital sovereignty" is uttered and this discourse's enabling and constitutive effects, precisely because of its conceptual ambiguity. Inspired by J. L. Austin's question, "how to do things with words" (Austin 1975), I analyze what actions and interactions of the EU and its interlocutors are enabled by the EU's invocation and pronouncement of "digital sovereignty".

While the speech act theory was initially developed by Austin in specific social linguist contexts, it has been imported to international relations scholarship, joining a rich body of constructivist and poststructuralist theories to explicate the processes in which the activity of speaking creates norms, self and collective identities, institutions and their environment (Müller 2011). Speech act theory has been used to analyse the construction of the European Union as a polity and the process of European integration (Diez 1999; 2001). In the field of security studies, explorations have been made into how the discourse and framing about security and fear are involved in a wide range of social and bureaucratic processes – known as "securitization" – that constitute security issues as well as security expertise (Huysmans 2006; Balzacq 2010). Building on the methodological moves of the existing IR scholarship, this paper looks at how discourses of the EU's digital sovereignty are connected to various state and EU practices and construct social reality about the EU and its relations to other actors.

In addition to speech act theory, I am particularly inspired by Hannah Arendt's political theory. Apart from her discussion on the performative dimension of speaking, which bears similarities with speech act theory, what is especially important here is that Arendt emphasizes the intersubjective character of speaking and acting (Arendt 1958, 179–80): these activities are always in front of others and in a context. "Others" are therefore an integral part of the performance (Loidolt 2018, 200). Drawing on her idea about the intersubjective nature of performance, I analyze the performance of the EU's discourse as co-performances between the EU and its interlocutors. This intersubjective nature of performance has an important

---

3 The GAIA-X project defines digital sovereignty as, "the possibility of independent self-determination by the state and by organisations with regard to the use and structuring of digital systems themselves, the data produced and stored in them, and the processes depicted as a result." (Federal Ministry of Education and Research 2019, 7) While this definition points to self-determination, the word "possibility" begs more questions about power, such as what the conditions of possibility are, who and how to identify and create the conditions of possibility.

4 For example, Krasner dismissed the normative or ideational conception of sovereignty and called it the "organized hypocrisy" (Krasner 1999, 24–25).

consequence, that is, the performance, as a lived experience in human togetherness, goes outside the intention and control of the initial performer. The speech becomes "unruly" (Constable 2014, 11), and the performer who utters the discourse becomes both "its actor and sufferer" (Arendt 1958, 184). This "unruliness" will be demonstrated later in the analysis which shows the various contradictions and tensions in the co-performances of digital sovereignty.

The emergence of the digital sovereignty discourse at the EU: an unusual return of geopolitics

Arguably, the EU's return to geopolitics started long before the recent pronouncement of digital sovereignty. One example of the EU dealing with geopolitics is the European Defence Action Plan proposed by the previous European Commission in November 2016 to attain strategic autonomy. The proposal was later adopted by EU leaders and contained, among other things, a European defence fund to support joint research and development of defence (European Commission 2016). From a realist point of view, it might be argued that geopolitical considerations never left the EU's agendas. Besides issues concerned with borders (such as eastern enlargement and migration), it has been argued that the EU's regulations and policies in the economic domain also concern its geopolitical leverages (Baun 1997; Butler 2011; Kupchan 2015). However, when it comes to the domains of data and the internet, the return of geopolitics as reflected in the EU's digital sovereignty discourse is quite special. This is partly because there is a strong ideological tendency of depoliticization in the domains of data and the internet, despite their clear connection with states' military power. Apart from the legacy of a whole generation of cyber libertarians that argued the internet was out of states' control (Barlow 1996; Johnson and Post 1996), two strands of international law have contributed to the depoliticization of "the digital"; international economic law, which portrays the digital economy as the object of next-stage liberalisation of the world economy (Gao 2018), and international human rights law, which is claimed to be applicable to the online as much as to the offline (Human Rights Council 2012).[5] Partly, the unusual nature of the discourse is due to the EU's own difficulties and reluctance to pronounce the word "sovereignty", and its commitment to the depoliticization of the digital, as we will see.

The EU's unusual assertion of digital sovereignty emerges from a combination of external and internal conditions that have made the depoliticization of "the digital" hard to withhold from the EU's perspective. I list these six conditions, commonly identified in policy papers:

1. American and Chinese big tech companies have largely dominated the European and global markets and elbowed out European companies. This domination is reflected not only in the market share of American and Chinese companies, but also in the number of patent applications and the amount of investments and R&D expenditure they achieve (European Political Strategy Centre 2019, 10–11; Joint Research Centre, 2019).
2. Accordingly, the EU and its member states are largely dependent on the services of foreign providers, especially in next-generation technologies, such as 5G and cloud computing, which could transform businesses and societies in unforeseen ways. Such technological dependency also extends to public sectors and strategically important areas with serious security implications.
3. Technological dependency and its social and security impact are considered detrimental to European democracy. Three kinds of democratic concerns are often mentioned: corporate power that surpasses the regulatory capacity of states is seen as anti-democratic, a relatively old charge against the tech giants; the development and deployment of certain technologies, typically artificial intelligence, pose challenges to

---

5 On the depoliticising effect of the human rights discourse, see e.g., (Douzinas 2007).

democratic principles and ethics; the threat to democracy has been more specifically identified with dis/misinformation on social media (mostly US media platforms) which have been profoundly involved in the spreading and shaping of political opinions.

4. At the international level, the EU's position, caused by its technological dependency, has become increasingly delicate because of the rising tensions between the US and China. In the high-tech sector, both the US and China see the European market as crucial for their economic and geopolitical interests. In the context of this trade war, the US has pressured the EU not to choose Chinese digital products and services, pushing the EU to be more dependent on American providers. However, the EU has also been forced to reconsider its partnership with the US, given the Trump Administration's attack on multilateralism and turn to protectionism in trade.

5. The EU's technological dependency becomes more problematic as the EU distrusts the protection of personal data in the US and China. The two countries are not considered by the EU to offer adequate levels of data protection.[6] This distrust is rooted in the surveillance practices of both countries and exacerbated by recently adopted laws in both countries, which extend the power of national authorities to have access to EU citizens' and business' data.[7]

6. The EU's technological dependency is accompanied by the fragmentation of its internal market and regulatory landscape, which has made endogenous businesses less competitive and the EU market less attractive for investment and restrained the EU's collective potential to develop digital capacity (Petit 2020).

These mixed conditions generate the EU's perceptions of its own vulnerabilities: losing the race in next-generation technologies, missing the critical opportunity of economic growth that those technologies would offer, lacking control and independence in determining the paths and the rules of digitalisation, and becoming the collateral damage in the techno-economic fight between the US and China. These perceptions are ultimately about existential threats and insecurity in both material and ideological senses. Threats to the security of data and digital infrastructures in Europe are seen to have the potential to cause significant economic and social costs, damaging European democracy and undermining values such as the sanctity of individual rights and the openness and fairness of the market economy.

The COVID-19 pandemic has aggravated these perceptions about Europe's vulnerability. Not only have US-China tensions worsened, the pandemic has also disrupted the global supply chains in many crucial industries and created enormous economic instability for the EU. A growing call for stronger governmental control over crucial supplies, such as medical equipment, shows that the EU's economic interdependence with others is now constraining its capacity to save lives. With respect to data and the digital infrastructures in particular, COVID-19 has created a strong push for a deeper and broader digital transformation of social activities and people's lives. This "mass migration" to online activity also made some of the pre-existing regulatory problems, such as privacy protection and regulation of mis/disinformation, more complicated to address in a piecemeal fashion. In addition to an increasing level of fusion between the online and the offline, digital technologies are also seen by many policymakers as providing solutions to COVID-19.[8] In such contexts, the control over data and digital infrastructures, to make sure they are secure, bears great and direct importance to COVID-19

---

6 The EU-US privacy shield was ruled invalid by the CJEU in Schrems II case on July 16, 2020. Case c-311/18.

7 The US CLOUD Act effectively gives a US court warrant to obtain electronic evidence extraterritorial validity; the Chinese National Intelligence law, article 7, creates legal obligations for every organization and citizen to support, assist and cooperate in national intelligence efforts. This would include Chinese companies doing business in the European market.

8 For example, it has been proposed to use AI for virus detection and blockchain for the management of medical data and medical supplies (Kritikos 2020)

management. Furthermore, COVID-19 presents a convincing case that data and digital infrastructures should be considered as a public good rather than the private properties of tech companies. In brief, in a time of greater geopolitical and social uncertainty, the technological dependency of European countries on foreign providers becomes increasingly a matter of existential importance. The vulnerabilities caused by such dependency could lead not only to losing the race to the US and China, but, more immediately, greater challenges for European countries in dealing with the pandemic. This latter consequence is clearly demonstrated by the controversy over centralised or decentralised systems of contact tracing apps.[9]

While the COVID-19 brought additional incentives, the EU and its member states have already been "at the forefront of almost all global regulatory endeavours aimed at checking the powers of digital giants" before the pandemic's outbreak (Christakis 2020, 16), often targeting US companies. There is a growing body of judicial decisions, regulations and legislative proposals that tackle issues ranging from the misuse of users' data,[10] to the abuse of market power,[11] to tax avoidance (European Commission 2018). In addition to taming the power of the big techs, there are also initiatives to strengthen Europe's capacity to control its datasphere and digital infrastructures, for example, the GAIA-X alliance led by Germany and France to create a federated and open data infrastructure for Europe. Some states, such as France, have also passed laws to require the sharing of data of public interest from the big techs to the government.[12] These moves all have geopolitical ramifications, but the geopolitical motivations have been less articulated,[13] as the EU more often stresses the protection of rights and interests of EU citizens and businesses. The Huawei saga is a notable change. Caught in the US-China trade war, the EU had to reconsider Huawei's status as a major 5G provider in Europe and asked the member states to strengthen and prioritize security requirements when assessing potential vendors (European Commission 2020a). The concern that the EU emphasizes, therefore, has shifted from mere technological dependency to threats to Europe's security, and the Chinese political system is often cited as a major risk factor (European Political Strategy Centre 2019, 16; Cerulus and Heikkilä 2020). This shift suggests a clearer turn to geopolitics in the digital and technological sectors by the EU.

Meanwhile, this change – i.e., towards greater assertion of sovereignty and a more explicit embrace of geopolitics – has happened and is still ongoing under a new European Commission, explicitly termed a "geopolitical Commission" by the president Ursula von der Leyen (Von der Leyen 2019a, 2). Unlike the previous commission, which adopted a more responsive and defensive tone when framing geopolitics,[14] von der Leyen has demonstrated a sort of will to power with European characteristics. In her speech in the European Parliament Plenary Session in November 2019, she said (Von der Leyen 2019b, 6), "The world needs our

---

9 For example, in praising the French app, Cédric O, French secretary of state for the digital economy, commented that "[a]t a time of domination by the GAFA…it seemed important to me to insist on the app's sovereignty" (Leprince-Ringuet 2020).

10 Most notably, the EU General Data Protection Regulation and the two Schrems cases.

11 E.g., Google Android (Case AT.40099) Commission Decision C(2018) 4761 final; Google Search (Shopping) (Case AT.39740) Commission Decision C(2017) 444 final.

12 French Loi pour une République Numérique 2016 gives municipalities the right to demand private operators to open their data, which are considered of general interest. These data include data from delegated public services, data essential for granting subsidies, and data needed for national statistics. Loi d'Orientation des Mobilités 2019 require mobility operators and some platforms to open static and real-time user information data.

13 Günther Oettinger's call for digital Europeanisation in 2015 is a rare case of explicit pronouncing of "digital sovereignty" by the EU before 2019 (Tost 2015).

14 In a brief on the European Defence Union, the Commission described the purpose of the 2016 European defence plan as "to defend her collective interests, respond to external conflicts and crises, and project security in our neighbourhood" (European Commission 2019, 1).

leadership more than ever. To keep engaging with the world as a responsible power. To be a force for peace and for positive change." This requires, she claimed (Von der Leyen 2019b, 9), among other things, "mastery and ownership of key technologies in Europe." Within the first 100 days, the new Commission set out a strategy for shaping Europe's digital future, a European strategy for data, and a White Paper on Artificial Intelligence. All these documents mentioned the term "technological sovereignty". On other occasions, the Commission has used the term "digital sovereignty" largely interchangeably with technological sovereignty (Madiega 2020; European Commission 2020d).

Von der Leyen's statement indicates that while external geopolitical conditions have forced the EU to speak the language of power, the discourse of digital sovereignty is more than responsive. As classical realist Hans Morgenthau argued, the instinct of self-preservation and the instinct to prove oneself are two fundamental drives of humans and groups (such as states) (Schuett 2010). While the discourse directly reacts to Europe's technological vulnerabilities, it signals the intention that the EU, by upholding its values, and in its quest for a "level playing field" and "strategic autonomy", aims to counter the existing domination of the US and China and the pulls of the geopolitical shifts and to offer a feasible alternative for the rest of the world. This ambition is demonstrated by von der Leyen's statement that "Europe will always lead the way when it comes to upholding and…updating the rule-based global order" (Von der Leyen 2019a, 4). And again, at the World Economic Forum in 2020, von der Leyen declared that "We need to rediscover the power of cooperation, based on fairness and mutual respect. This is what I call 'geopolitics of mutual interests'" (Von der Leyen 2020a). Making "a Europe fit for the digital age" is inseparable from making the digital age fit for Europe. Therefore, the EU's discourse of digital sovereignty will have broader consequences for the global digital environment. This outward-looking ambition, inherent to the assertion of sovereignty, is made explicit in some policy discussions. For example, a paper by the European Political Strategy Centre entitled "Rethinking Strategic Autonomy in the Digital Age" claims that the traditional defence-centered understanding of strategic autonomy is insufficient and needs to be broadened in the context of hyperconnectivity and digitalisation (European Political Strategy Centre 2019, 2). Depending on the geopolitical position of the audience, the EU's sovereignty discourse may even be interpreted as offensive. Be that as it may, self-empowerment by a polity will always have broader, external consequences. For the EU, this spillover effect is already reflected in the extraterritorial character of its data protection framework, even before the term of digital sovereignty gained traction in the EU.

Discursive co-performances of EU digital sovereignty

As mentioned earlier, this paper sees "digital sovereignty" as discursive performance: as it is made in the presence of particular audiences, appeals to them and is interpreted by them, the performance is always co-performance. The intersubjectivity of performance is well explored in Arendtian political philosophy (Arendt 1958). Here, I look at three co-performances enacted through the EU's discourse of digital sovereignty: the first two are by different polities at international and European levels; the third is between the EU and rights advocates.

co-performance, part 1: mimesis and potential moving beyond
Given the geopolitical conditions that paved the way for the EU's digital sovereignty discourse, what this discourse does, first, is to identify existential threats from the outside that both the EU and its member states need to tackle in the digital age. Most of the policy debates at the EU quite frankly acknowledge external existential threats, for example, claiming that "the US is the biggest problem, China has become the biggest fear" (Shapiro 2020, 10). This more outward-looking dimension of the sovereignty discourse, compared to the inward-looking question about the EU's constitutionalism or democratic foundation, reflects the EU's move

toward speaking more clearly the language of power. The audience and interlocutors here are those who have posed existential threats to the EU, and they are an integral part of the EU's invocation of digital sovereignty. As referred to earlier, the EU's turning to geopolitics in some ways mimics its external competitors.

Mimesis is an old and pervasive phenomenon in human collective behaviours and has only lately attracted the attention of scholars of international relations and political theory, inspired by René Girard's mimetic theory (Farneti 2015; Brighi and Cerella 2015; Troy 2015). For the purpose of this essay, I borrow insights from mimetic theory for observing and interpreting empirical phenomena, rather than delving into its more profound restructuring consequences for political ontology and epistemology. For this co-performance, I discuss two EU mimetic relationships: with China and with the US.

Regarding the first mimetic pair, looking at the emergence of the digital sovereignty discourse in the EU, it is impossible not to notice that the very sovereignty framing with respect to the digital sphere and infrastructure already shows a striking similarity with the Chinese approach to data and internet governance. However digital sovereignty and cyber sovereignty are understood by the EU and China, a common characteristic between the two is the rhetorical strategy that exploits conceptually highly contentious and ideologically (and emotionally) charged concepts.

In addition to this rhetorical mimicry, several policy initiatives have been brought under the scope of EU digital sovereignty, which seems to suggest this trend of "Chinafication of EU industrial policy" (Bauer 2020). One is the recent rise of (neo)mercantilism to back up the sovereignty discourse at the EU, which resembles the mercantilist tradition in China (as well as the trend in the US, see below). The close relationship between the Chinese government and the private sectors – as traditionally expressed by the state-owned-enterprises and industrial subsidies – is well-known. While depicted by the EU as major anomalies disqualifying China from having market economy status and contributing to the EU's grievances about its imbalanced and unfair relationship to China (European Parliament 2016; Emmott and Blenkinsop 2020), the Chinese strategies of developing technological and industrial self-reliance are selectively, but increasingly, picked up by the EU: prime examples are the effort to more forcefully direct and mobilize public and private investment to R&D for next-generation technologies and to more closely connect digitalisation and technological innovation with social developmental goals.[15]

In addition to supporting European industries, several initiatives point in the direction of data localization, which shows the tendency to imitation more clearly. Conceiving data as industrial assets, Thierry Breton, the Commissioner for Internal Market, commented, "The Chinese and the Russians are doing it, we will do it too" (Christakis 2020, 65). Regarding the transfer of non-personal data to third countries, the current version of the Data Governance Act allows the Commission to assess the level of data protection offered by third countries and to adopt special requirements for the transfer of "highly sensitive" non-personal data held by public sectors.[16] While refraining from a default data localization rule, the protection mechanism provided by the Act arguably amounts to the so-called "soft data localization" (Chander 2020), of which the practical consequence could be similar to that of China's Cybersecurity Law.[17]

---

15 According to the EU Multiannual Financial Framework 2021-2027, over 50% of the 1.8 trillion euros goes to modernisation, which includes research and innovation and fair climate and digital transitions.

16 Data Governance Act, art. 5(9), 5(11).

17 The Chinese cybersecurity law imposes security assessments by the state authorities for the cross-border transfer of personal and important data held by critical information infrastructure operators. China cybersecurity law, art. 37.

The mimesis with the US is twofold: first is the mimetic rivalry similar to that with China, and the second is a kind of mimetic alliance with the US against China. Regarding the former, as in the case of mimesis with China, the increase in public and private financing for the tech sectors by the EU and the construction of a single digital market are strategies of imitating the US to strengthen European digital capacity against domination by American big techs. This kind of mimicry with the US has been demanded for quite some time by European private sectors who are highly critical of the EU's fragmented business and investment environment and its burdensome regulatory frameworks and jealous of those of the US (Pethokoukis 2016). The mimetic alliance between the EU and the US against China is manifested by the rise of mercantilism on both sides of the Atlantic. In the US, laws and executive orders, applying security framing, have been used against Chinese telecom exports and investment in the US in sectors considered sensitive. The US's security framing and its Huawei ban have had a significant contagious effect. For example, Theodore Christakis argues that, since the American big techs consider China's potential leadership in AI a security threat for the world, "how on earth could [the European leaders] do otherwise" (Christakis 2020, 42). And indeed, the EU's foreign investment screening and public procurement rules now emphasize security criteria, which largely target the Chinese telecom companies (European Parliament and the Council 2019; European Commission 2020a, SA10).

This is not to say that it is only the EU that is imitating the others. Imitation has contagious and sometimes escalating effects, and the relationship between the US and China clearly demonstrates this vicious cycle. As the EU takes a more assertive geopolitical position, what can reasonably be expected is that its sovereignty discourse will be interpreted by its audiences from their own perspectives and inform their actions. So far, the sovereignty discourse has alerted commentators in the US, warning that if the EU continues asserting its digital sovereignty, "US policymakers will have no choice but to treat it as a strategic threat". (Barshefsky, 2020) In China, the EU's discourse is interpreted in two ways. It is seen as a signal of the EU's growing distrust of China, or as an endorsement and reinforcement of China's sovereigntist approach to cyberspace governance. In both ways, scholars argue that the EU's move creates more demands and opportunities for China-EU dialogue and consensus building to forge an anti-US alliance (Jin 2020; Wu 2020; Lu and Fan 2020). Such interpretation, if put in practice by Chinese policymakers, would run largely contrary to the EU's initial intention of getting out of US-China crossfire.

The interpretation by Chinese scholars exploring potential for China-EU cooperation and consensus points to an interesting aspect of imitation. While Girard and the IR drawing on him often emphasize the relationship between imitation and conflict, imitation also generates agreements and consensus.[18] Arguably, the somewhat familiar "sovereignty" language (whether the EU would agree) would incentivise China to "learn from" the EU's regulatory design for digital technologies to improve its own governance frameworks and to make regulatory "interoperability" between the two more possible (Wu 2020; China Industrial Information Security Development and Research Centre 2020). Such potential consensus building could be even more likely for the transatlantic relationship in the post-Trump era. However, conditions for having such positive effects of imitation are largely constrained by overarching geopolitical shifts.

For the EU, and except for those politicians who claim that "we will do it too", imitation with external competitors is not something that can be proudly acknowledged, but rather something to be avoided. Many commentators consider the EU's tendency to imitation as irrational and

---

18 Albeit according to Girard, this agreement and consensus formation is a result of the scapegoat mechanism that unites the imitating actors and directs their hostility toward a common enemy. See (Johnston 2014).

economically harmful (Burwell and Propp 2020, 6; Christakis 2020, 67; Bauer 2020). Especially with respect to China, the EU is hasty to emphasize the difference: the uniqueness of the EU's approach, it claims, lies in European values and interests. European enlightenment values, in particular, are often singled out to distinguish the EU's approach from the authoritarianism and collectivism of the Chinese. Some criticisms against the regulatory initiatives that move toward data localization are made precisely on the grounds of European uniqueness; that is, the EU should not send the signal of approving the policies of those countries that are authoritarian or less democratic than the EU (Global Data Alliance 2020).

Similarly, the EU differentiates itself from the US's Trumpism, which is seen as a betrayal to multilateralism. These differences of values are essentially identity markers that are hugely important for the EU's self-understanding and for justifying its resort to sovereignty. However, can the affirmation and reinforcement of European uniqueness pull the EU out from the mimetic loops? A Girardian answer would be no. From a mimetic perspective, the EU's reinforcement of its differences is always what adversaries in mimetic rivalry do; the adversaries would never acknowledge they are just copycats of each other. To use Girard's words (Girard 2009, 14), the mimesis "can be seen only by someone who is outside the conflict because *from the inside you must always believe in your difference*… From the outside, the adversaries look like what they are: simply doubles." Reassuring one's distinctiveness is the reaction that compensates the loss of identity caused by increasing "undifferentiation"(Girard 2005) so that imitation could continue (Girard 2009, 88; Farneti 2015, 30).

Of course, these apparent imitations do not mean that the EU is stuck in mimetic loops with the US and China. From the perspective of mimetic theory, the consequence of such loops would be destructive, leading to a sort of explosion of mimetic violence.[19] For the EU, the more immediate issue raised by mimetic relationships is that such relationships could seriously undermine one's autonomy. This is because precisely through imitating the other's desires, attitudes and strategies, by becoming the copycat, one loses one's autonomy (Farneti 2015, 10). This consequence that mimetic theory illuminates could undermine the EU's explicit objective to achieve strategic autonomy when joining this geopolitical game. Therefore, it is critically important for the EU to transcend the mimetic imperative, but whether the digital sovereignty discourse offers such a possibility is, at best, an open question.

co-performance, part 2: ostensible convergence between the EU and member states

The co-performance at the European level touches upon foundational questions about the EU: on what grounds can the EU, as a transnational polity, invoke sovereignty, however vaguely defined? How to position digital sovereignty in the current legal and political structure that divides sovereign powers between the EU and its member states? These foundational questions are also the reason why speaking of digital sovereignty poses particular problems for the EU. Indeed, before the recent return of geopolitics, it was rare for the word "sovereignty" to be pronounced so loudly by the EU. The EU's authority has been more commonly discussed in terms of regulatory competence or administrative power, with emphasis put on expert authority rather than sovereignty. A huge body of literature has explored the theoretical conundrum about the "divided and pooled sovereignty" of the EU (Majone 1998, Gerstenberg and Sabel 2002, Fichera 2018). Apart from the academic debate over the conceptual value of the word "sovereignty" in the structure of transnational governance, a series of crisis that exposed the EU's democratic deficits have been responded by strong reaffirmation of state

---

19 Girard (2005) calls this the sacrificial crisis where the imitation escalates to the extent that violence is so widespread, all differences are eliminated, and all animosity converges against a third party, a sacrificial victim.

sovereignty by Eurosceptic or populist governments and parties (not only in the east Europe, but also in the west as notably seen in the Brexit). Against this political background of the EU struggling with its democratic legitimacy, such an explicit invocation of digital sovereignty by the EU appears a striking response to various political temptation of exiting the EU.

In the current geopolitical contexts that give rise to the digital sovereignty discourse, the co-performance at the EU level has less, for the moment, to do with dividing regulatory competences between the EU and its member states, and more with mobilizing concerted and coordinated efforts in the region to redress its disadvantages vis-à-vis the US and China and the vulnerabilities caused by the region's dependency on foreign technological and economic supplies. The reflexive effect of the co-performance with foreign competitors is clear: the construction of external existential threats simultaneously constitutes a collective that perceives and responds to the threats in a unified way. The EU's invocation of digital sovereignty is therefore also a process of collective self-identification, by which Europe proudly affirms its approach to digitalisation and data governance in a more powerful tone; "this is about Europe shaping its own future" (Von der Leyen 2020a) and "We want to lead the way, the European way, to the Digital Age: based on our values, our strength, our global ambitions" (Von der Leyen 2020b). The EU's approach, contra that of the US or China, is uniquely European, a sort of "enlightened capitalism", which embraces both the logic of the market (hence, the principles of openness and competition) and enlightenment values such as individual rights, democracy and the rule of law. A successful co-performance with the external competitors in the geopolitical game is predicated on an effective co-performance within Europe: the discourse of digital sovereignty bolsters European collective self-identification by facilitating the EU's new industrial policies, investment priorities and regulatory frameworks to harness and direct social and financial resources from its member states and various sectors to develop European digital capacity and to compete for global innovation leadership (World Economic Forum 2019). Meanwhile, this process of collective self-identification also presumes that interests and values of different groups within Europe share enough common ground. The construction of common interests and values and the identification of common threats may reasonably initiate and legitimate new measures toward European integration.

The line between politicisation and geo-politicisation hence becomes blurred. The outward-looking dimension of the sovereignty assertion would inevitably have ramifications for the EU's internal politics. It is too early to say whether the EU's digital sovereignty discourse will somehow lead to a greater level of sovereign power transferred from the member states to the transnational body, or how exactly the EU's digital strategies will be implemented in accordance with the principles vital to EU law, such as subsidiarity and proportionality. At the moment, the digital sovereignty discourse is co-performed within the EU by many member states, endorsing and supporting a greater role of the EU in setting out the collective digital future for the region. These states typically find themselves incapable of addressing the problem of technological dependency and associated security risks alone and consider coordinated EU-wide solutions necessary, because of the hyper-connective nature of those risks (European Commission 2020c, 22–23, 29–30). In addition, state-led initiatives that are formulated by similar sovereignty discourses, such as the GAIA-X project, are presented as compatible with the Commission's goal and are open to the projects of the Commission (Federal Minsitry of Education and Research 2019, 14). In various settings, the digital sovereignty discourse is pronounced by both member states and the Commission. This co-performance of digital sovereignty is also related to a recent change in Europe where states, like Germany, traditionally skeptical about mercantilism, are becoming increasingly active in protecting and empowering their strategically important sectors (Warlouzet 2020). A significant convergence of interests between these states and the EU leads to a choir singing sovereignty, and the EU and the member states take and occasionally switch between soprano and bass and lend support to each other. The EU gains more legitimacy thanks to the states' support,

and member states' voices become less nationalist and more European than they might otherwise sound.

How coordinated this choir can be remains a big question. Dissonances within the choir of digital sovereignty are not unlikely, given that the societal scale of digitalisation raises many political problems sensitive to states' interests and identities. Some early signs of potential dissonances can be gleaned from the issue of 5G technology standards. Developing and promoting European 5G standards is a quintessential regulatory issue and an integral aspect of the EU's digital sovereignty (European Commission 2020b, 16), which is however said to be considerably impeded by the internal fragmentation of the EU's telecommunication market (Duchâtel and Godement 2019, 17). While a coordinated EU-wide approach to 5G network security is called for by the European Commission (European Council 2020, para. 11) and some member states (European Commission 2020c, 29), the manner in which 5G is to be rolled out remains a political question for individual member states and cannot be imposed by the EU. In addition, as 5G is perceived to have serious national security implications, the fact that the EU has no legal authority to regulate national security issues further complicates the internal fragmentation.[20] This is reflected in the inconsistencies of EU countries' positions on the Huawei problem. It remains highly questionable whether the discourse of EU digital sovereignty could entail an increased level of EU intervention in the national security matters of its member states.

Internal fragmentation is further seen in the unequal political and economic power among EU countries. Behind the hype of the collective self-identification for a European digital future, a legitimate question would be: what is "our industry"? The main vocal proponents of EU digital sovereignty, i.e., Germany and France, are also the largest EU economies. At a superficial level, sovereignty discourse totalising the interests of member states could end up strengthening their domination in the European market, while undermining other member states' opportunities to develop their own digital capacities (Schadt and Zobel 2020). Indeed, several EU countries have expressed suspicion that the EU's digital sovereignty would lead to protectionism favouring only Franco-Germany industries at the expense of smaller economies (Tamma 2020; Bauer and Erixon 2020, 2–3). At a deeper level, whether and how to distribute the economic gains of a state's domestic industry beyond the degree of self-sufficiency and their spillover social benefits in a manner that strengthens the whole region remains an unaddressed political question.

co-performance part, 3: the question of individual digital sovereignty

While the two co-performances discussed in the preceding subsections focused on the actions of polities, here, I look at that between the EU and a particular constituent of the European public, rights advocates. This co-performance raises a critical question about the relationship between the discourse of the EU's digital sovereignty and the notion of individual digital rights. To put it bluntly, if European digital sovereignty is construed as encompassing the protection of individual rights, then its distinctiveness vis-à-vis Chinese cyber sovereignty, which is rhetorically conceptualized as incorporating the protection of the people's rights and interests (Xu 2017), may appear less self-evident and would need significant elaboration.

This question is important for both the EU and the field of data and internet governance. Both the EU and the mainstream scholarship in data and internet governance share strong skepticism about sovereignty. A discourse of sovereignty typically sets off an alarm to those who consider liberal values and principles (e.g., free flow of data, decentralisation, individual

---

20 Art 4(2) of the Treaty on EU.

rights, multistakeholderism) to be crucial for the governance of data and cyber affairs (Mueller, 2020). The fact that Russia and China have adopted a sovereigntist approach to internet governance is an important contributing factor to this skepticism, which often relates sovereignty discourses to issues such as data localisation, technological protectionism, the infringement of freedom of expression and the balkanisation of the internet. At various governance and negotiation fora, the EU has committed itself to liberal principles and opposed the sovereigntist approach to governing cyber affairs (European Commission 2014; Council of the European Union 2014). Up till now, the growing regulations it has imposed on big techs are typically framed in a rather apolitical way: the EU often portrays the object and purpose of the regulatory power as the restoration of competition in the market or as the protection of consumer rights and individual fundamental rights. In particular, rights protection has been the dominant European approach to governing big techs and data.

In this general context of sovereignty skepticism, this third co-performance would involve some significant reconciliation between the rising sovereignty discourse at the EU and the notion of individual digital rights. It is interesting to see how advocates in Europe for privacy and data protection have started incorporating the term "digital sovereignty" and read individual rights into it without much difficulty. This reinterpretation of sovereignty is supported by the European Commission. One example of such reinterpretation can be seen in a plenary session themed "Digital sovereignty – from users' empowerment to technological leadership", co-organized by the European Commission at the European Dialogue on Internet Governance in June 2020 (EuroDIG 2020). The panel construed digital sovereignty as twofold, comprising users' digital sovereignty, in terms of individual control over personal data and digital identity and exercising digital self-determination, and Europe's strategic autonomy in the technological supply chain, with the two aspects being considered complementary (O'Donohue 2020). Attaching the protection of individual rights to EU digital sovereignty is an interesting case of "(re)branding". Before the notion of digital sovereignty became popular at the EU in 2019, it was rarely used as a catchall phrase for individuals' digital rights.[21] For example, going through the legislative history of the GDPR from 2013 to 2016, no mention of digital sovereignty or individual sovereignty can be found in the positions of the EU Council and debates at the European Parliament; the term in discussions was "fundamental rights" (Council of the European Union 2014; 2016a; 2016b).

Individuals' digital rights, as well as the underlying notion of informational self-determination (Rouvroy and Poullet 2009), are now reframed as "users' digital sovereignty". However, the seemingly terminological change can entail something significant. This paper is not the place for a thorough examination and critique of individual digital sovereignty. It suffices to briefly mention two issues. First, individual digital sovereignty is sometimes conceived by seeing individuals as consumers (Pohle & Thiel 2020, 12). However, the empowering effect of consumer sovereignty is at best highly controversial (Swyngendouw 2005; Clarke 2011; Hammett 2018). Second, if seeing individuals primarily as political agents, individual digital sovereignty points to a recurrent question in constitutional democracy regarding the relationship between individual self-determination and collective self-government (e.g., Habermas 1996). To "appropriate" the discourse of digital sovereignty so that the rights advocates could have a voice in performing the EU's digital sovereignty discourse, what they do at best is to juxtapose individual sovereignty with collective sovereignty (i.e., "European sovereignty", quietly skipping state sovereignty) and present the two as somehow logically

---

21 Exceptional use of the word sovereignty can be found in the work of Shoshana Zuboff (2019) and of Luukas Ilves and David Osimo (2019) where individual/personal sovereignty is used as a catchall term for individuals' digital rights, but they do not discuss the theoretical underpinning of the idea. It is also used by Julian Gill-Peterson (2015), who conceives the user's technological sovereignty through the lens of bodily sovereignty when the user engages in the practice of sexting.

linked without any explanation. This is evident in the "Digital Sovereignty" panel mentioned earlier. The complementarity between the two aspects – users' digital sovereignty and European strategic autonomy – is assumed rather than examined. While the connection between the two may be theorized from the lens of popular sovereignty, that connection inevitably opens up questions about political representation and authorization, i.e., who is acting on behalf of individuals and on what ground (Lindahl 2018). Understandably, addressing these questions is beyond what rights advocates usually do. However, as Palantir (the US company that cooperates closely with the US military and intelligence services) has joined the GAIA-X, we might wonder whether rights advocates would still combine individual digital sovereignty with EU digital sovereignty without much reservation.

Conclusions

The discourse analysis offered by this paper, and especially the examination of the three co-performances, displays various tensions and contradictions that condition how "digital sovereignty" is pronounced, received and responded. Accordingly, the discourse, as co-performance, also influences the relations between the EU and its interlocutors. For the EU's objective of increasing strategic autonomy and becoming more self-reliant, the analysis shows that the discourse of digital sovereignty can lead to counterproductive and even self-defeating effects. The apparent geopolitical conditions that have pushed the EU to assert its digital sovereignty simultaneously constrain how the sovereignty discourse can be deployed creatively. The perception of the EU's vulnerability is largely relative to what the US and China have or desire to have, and by comparing itself to the US and China, the EU enters into mimetic relationships with the other two and is significantly influenced by their outlooks, strategies and attitudes. Analyzing from the perspective of mimetic theory, it can be argued that imitation not only does not resolve the competition between rivals, but more importantly can defeat the very purpose of the EU to achieve self-reliance and strategic autonomy. The identification of, and emphasis on, European distinctiveness do not matter that much, because, again from a mimetic perspective, it is the process of imitation that leads to the compensation by resorting to identity markers, i.e., European values and principles. Upholding identity markers, in turn, makes the imitator less disturbed by the undifferentiating effect of imitation and allows the imitation to continue. To liberate oneself from the mimetic relationships, it is perhaps less useful to keep talking about "the European way" and "our values", than to acknowledge and confront more directly the kneejerk impulse of imitation as expressed by the EU's turn to "sovereignty" framing.

At the European level, this discourse has reflexive effects and appeals to the EU member states in order to push forward new dimensions of European integration and to make the digital sovereignty discourse a concrete reality. This EU discourse is co-performed by the member states offering their endorsement, but potential setbacks are possible because fundamentally theoretical and political questions about how to understand sovereignty in the EU structure are left untouched. Finally, the discourse also appeals to and engages rights advocates. This leads to an uneasy reconciliation between the EU's tradition of sovereignty skepticism and rights protection on the one hand and the need to speak the language of power on the other. Here, the co-performance is notably done by the rights advocates appropriating the sovereignty discourse, which in fact reveals, rather than solves, the difficulties of this reconciliation. These questions may get fleshed out through longer-term co-performances by relevant actors, no longer glossing over conceptual uneasiness and political tensions.

Given the apparent universal ambition of the EU "to become a force for peace and positive change", it may still be interesting to consider how the EU's sovereignty can be deployed not simply to emulate and to compete with the US and China, but to join and inspire various

sovereignty assertions of other actors, be they states from the Global South or non-state actors such as indigenous peoples. Rather than aligning these different groups with a totalising notion of digital sovereignty with predetermined definition, the sovereignty discourse may be purposefully and creatively "misused" for the objective of resisting the hegemonic tendencies of the US and China and countering the domination of their tech companies.

References

Arendt H (1958) *The Human Condition*. Chicago: University of Chicago Press.

Austin JL (1975) *How to Do Things with Words*. Clarendon Press.

Balzacq T (2010) *Securitization Theory: How Security Problems Emerge and Dissolve*. Routledge.

Barlow JP (1996) A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. February 8, 1996.

Barshefsky C (2020) EU digital protectionism risks damaging ties with the US. Financial Times. August 2, 2020.

Bauer M (2020) Calls for Chinese-Style Tech Industrial Policy Won't Make Europe More Digital Sovereign. European Centre for International Political Economy. September 2020.

Bauer M and Erixon F (2020) Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls. 02/2020. ECIPE Occasional Paper. European Centre for International Political Economy.

Baun M 1997. The Geopolitics of European Monetary Union. *Southeastern Political Review* 25 (2): 281–302.

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

Brighi E and Cerella A (2015) An Alternative Vision of Politics and Violence: Introducing Mimetic Theory in International Studies. *Journal of International Political Theory* 11 (1): 3–25.

Burwell FG and Propp K (2020) The European Union and the Search for Digital Sovereignty Building Fortress Europe or Preparing for a New World. Atlantic Council.

Butler E (2011) The Geopolitics of Merger and Acquisition in the Central European Energy Market. *Geopolitics* 16 (3): 626–54.

Cerulus L and Heikkilä M (2020) EU Lawmakers Brand Huawei, ZTE 'High-Risk' 5G Vendors. POLITICO. October 14, 2020.

Chander A (2020) Is Data Localization a Solution for Schrems II? *Journal of International Economic Law* 23 (3): 771–84.

China Industrial Information Security Development and Research Centre. 2020. "欧盟争夺数字主权的最新进展及对我国的启示 [The Latest Development of EU Struggling for Digital Sovereignty and Its Implications for China]." MGClouds. March 12, 2020. https://www.mgclouds.com/archives/9883.

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.

Clarke J (2011) Citizen-Consumers: Hyphenation, identification, Depoliticization? In Brückweh K (ed), *A History of Market Research, Consumer Movements, and the Political Public Sphere* Oxford University Press, pp. 225–242.

Constable M (2014) *Our Word Is Our Bond: How Legal Speech Acts*. Stanford University Press.

Council of the European Union (2014) Council Conclusions on Internet Governance. Brussels: European Union.

Council of the European Union (2016a) Statement of the Council's Reasons: Position of the Council at First Reading with a View to the Adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

Council of the European Union (2016b) Legislative Acts and Other Instruments: Position of the Council at First Reading with a View to the Adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the Protection of Natural Persons with Regardto the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

Delcker J (2019) Germany's Plan to Control Its Own Data. POLITICO. September 12, 2019.

Demchak CC and Dombrowski P (2011) Rise of a Cybered Westphalian Age. *Strategic Studies Quarterly* 5 (1): 32–61.

Diez T (1999) Speaking 'Europe': The Politics of Integration Discourse. *Journal of European Public Policy* 6 (4): 598–613.

Diez T (2001) Europe as a Discursive Battleground: Discourse Analysis and European Integration Studies. *Cooperation and Conflict* 36 (1): 5–38.

Douzinas C (2007) *Human Rights and Empire: The Political Philosophy of Cosmopolitanism*. Routledge-Cavendish.

Duchâtel M and Godement F (2019) Europe and 5G: The Huawei Case. Institut Montaigne.

Emmott R and Blenkinsop P (2020) 'We Won't Be Played', EU Tells China's Xi. *Reuters*, September 14, 2020.

EuroDIG. 2020. *Digital Sovereignty – from Users' Empowerment to Technological Leadership*. https://eurodigwiki.org/wiki/Digital_sovereignty_%E2%80%93_from_users%E2%80%99_empowerment_to_technological_leadership_%E2%80%93_PL_02_2020.

European Commission (2014) European Commission Position for Internet Governance Forum 2014. September 2, 2014.

European Commission (2016) European Defence Action Plan: Towards a European Defence Fund. November 30, 2016.

European Commission (2018) Proposal for a COUNCIL DIRECTIVE Laying down Rules Relating to the Corporate Taxation of a Significant Digital Presence." COM(2018) 147 final. Brussels.

European Commission (2019) Towards a European Defence Union: Towards a More United, Stronger and More Democratic Union.

European Commission (2020a) Cybersecurity of 5G Networks - EU Toolbox of Risk Mitigating Measures.

European Commission (2020b) A European Strategy for Data (COM(2020)66 Final).

European Commission (2020c) Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity.

European Commission (2020d) Europe: The Keys To Sovereignty. September 11, 2020.

European Council. 2020. "European Council Conclusions EUCO 13.20 of 1st/2nd October 2020 Special Meeting." European Council.

European Parliament (2016) European Parliament Resolution of 12 May 2016 on China's Market Economy Status (2016/2667(RSP)).

European Parliament and the Council (2019) Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 Establishing a Framework for the Screening of Foreign Direct Investments into the Union. Official Journal of the European Union.

European Political Strategy Centre (2019) Rethinking Strategic Autonomy in the Digital Age. EPSC Strategic Notes. European Commission.

Farneti R (2015) *Mimetic Politics: Dyadic Patterns in Global Politics*. Michigan State University Press.