European Security

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/feus20

Digital/sovereignty and European security integration: an introduction

Rocco Bellanova, Helena Carrapico & Denis Duez

To cite this article: Rocco Bellanova, Helena Carrapico & Denis Duez (2022) Digital/sovereignty and European security integration: an introduction, European Security, 31:3, 337-355, DOI: 10.1080/09662839.2022.2101887

To link to this article: https://doi.org/10.1080/09662839.2022.2101887

Published online: 09 Sep 2022.

EUROPEAN SECURITY
2022, VOL. 31, NO. 3, 337–355
https://doi.org/10.1080/09662839.2022.2101887

Routledge
Taylor & Francis Group

Digital/sovereignty and European security integration: an introduction

Rocco Bellanova [a,b], Helena Carrapico[c] and Denis Duez [b]

[a]Department of Media Studies, University of Amsterdam, Amsterdam, The Netherlands; [b]Institute for European Studies, Université Saint-Louis, Bruxelles, Belgium; [c]Department of Social Sciences, Northumbria University, Newcastle upon Tyne, UK

ABSTRACT

The notion of *digital sovereignty*, also often referred to as *technological* sovereignty, has been gaining momentum in the European Union's (EU) political and policy discourses over recent years. Digital sovereignty has come to supplement an already substantial engagement of the EU with the digital across various security policy domains. The goal of this article and of the overall Special Issue is to explore how the discourse and practices of digital sovereignty redefine European security integration. Our core argument is that digital sovereignty has both direct and indirect implications for European security as the EU attempts to develop and control digital infrastructures (sovereignty *over* the digital), as well as the use of digital tools for European security governance (sovereignty *through* the digital). It is thus essential to further explore digital sovereignty both in terms of European policies and of a re-articulation of sovereign power and digital technologies – what we suggest calling *digital/sovereignty*.

ARTICLE HISTORY
Received 1 December 2021
Accepted 12 July 2022

KEYWORDS
Digital sovereignty; European security integration; technology; infrastructure; Sovereign Power

Introduction

Digital data and technologies have become key to the process of European Integration. The 2019–2024 European Commission (von der Leyen, 2019) and the European Council (2020) increasingly spearhead digital technologies as both a crucial site and a tool for European Union (EU) governance. At the heart of many initiatives lies the notion of *digital sovereignty*. The President of the European Commission, the President of the European Council and the High Representative of the Union for Foreign Affairs and Security Policy all referred to it in public speeches between 2019 and 2022. At first sight, this term leverages on a traditional notion of modern statecraft (Bellamy, 2017) and invokes a socio-technical imaginary of technological innovation (Jasanoff and Kim, 2015). Dubbed "technological sovereignty" at times, through this term the Commission vocalises its ambitions for further European integration in the twenty-first century (EC, 2020c, p. 2). Digital sovereignty is presented as the way forward to developing the EU as a secure and resilient society, to achieving a leadership position within the international system and

CONTACT Rocco Bellanova r.bellanova@uva.nl

reducing its dependence on other parts of the world. Digital sovereignty thus becomes a form of strategic autonomy from third countries and re-orienting relations with "Big Tech", notably through the creation of EU's own digital infrastructures. Digital sovereignty also complements the concept of "European strategic autonomy" proposed in the past by the European Council on Foreign Relations (Mogherini, 2016), and recently relaunched in the context of the COVID-19 pandemic (Borrell, 2020, Michel, 2021). Strategic autonomy implies that the EU and its Member States must preserve for themselves the ability to act in a deeply interdependent world.

This Special Issue aims at exploring how the discourses and practices of digital sovereignty redefine European security integration. Our core argument is that digital sovereignty has both direct and indirect implications for European security. It concerns the EU's attempt to develop and control digital security infrastructures, which we call sovereignty *over* the digital, but also the use of digital technologies for European security governance, which we contrast as sovereignty *through* the digital. Both dynamics have an impact on the practice of European security, as well as the nature of European security integration. For instance, the EU is gradually embedding cyber security instruments across all its policy areas. At the same time, the creation of new databases and connections between them and existing ones show that European policy-makers are very aware of the role of digital infrastructures in crucial domains such as counter-terrorism and border controls. Yet, we argue that looking at these policies only in terms of radical discontinuity with the past risks being shortsighted. Hence, we believe that it is essential to further explore digital sovereignty also in the broader terms of a re-articulation of sovereign power and digital technologies. This is what we suggest calling digital/sovereignty. The slash between the two terms invites us to better grasp not only specific policies but the deeper dynamics at play in the reconfiguration of modern power relations, which can be hardly separated – in practice – from the design, use and control of digital technologies. This approach is particularly promising if we are to unpack European security integration. In fact, discussions on the concept of digital sovereignty are gaining traction across diverse disciplines (e.g. Floridi, 2020, Pohle and Thiel, 2020) and in the policy literature (Hobbs, 2020). Yet they remain underexplored in European security literatures because the institutional jargon of European digital sovereignty is not yet mainstream in related policy domains (with the partial exception of cybersecurity).

By focusing on the nexus between digital/sovereignty and European security integration, this Special Issue raises questions about what kind of security actor the EU wants to become (Barrinha and Christou, this issue, Farrand and Carrapico, this issue), what strategy and practices the EU is developing to achieve its vision (Lambach and Monsees, this issue, Calderaro and Blumfelde, this issue), what security politics underpin European initiatives in the digital realm (Bellanova and Glouftsios, this issue, Oliveira Martins, Lidén and Jumbert, this issue) and how power relations are redefined across Europe. When we place digital sovereignty against a background of increased geopolitical competition and of a spreading datafication of our societies, such developments raise important questions regarding how digital technologies shape our societies and challenge fundamental rights (Oliveira Martins, Lidén and Jumbert, this issue), who produces and controls digital infrastructures and how data processing practices are regulated (Farrand and Carrapico, this issue, Bellanova and Glouftsios, this issue, Oliveira Martins, Lidén and Jumbert, this issue). By tackling these questions, this Special Issue supplements

a growing wealth of scholarly conversations across those European security literatures attentive to the policy and power dynamics underpinning police cooperation and counter-terrorism (de Goede, 2012, Bigo, 2014, Kaunert and Léonard, 2019), cybersecurity (Christou, 2016, Carrapico and Barrinha, 2017, Christou, 2019) and the increasing role of digital technologies in the European security landscape (Bellanova and Duez, 2012, Bossong and Carrapico, 2016, Calcara *et al.*, 2020).

Our Special Issue adopts a pluralistic, transdisciplinary ethos. Besides its policy salience, tackling European digital sovereignty means discussing anew terms – digital and sovereignty – that haunt and inform research across Political Science, International Relations, Law, International Political Sociology and Science and Technology Studies (STS). This is what we do in this introductory article, by creating a dialogue between them, and thus pondering their supposed foundational value and their potential conceptual momentum. In the same spirit, rather than imposing a single theoretical framework across the Special Issue, we want to foreground the epistemic richness to be gained in adopting diverse disciplinary and epistemic approaches, ranging from more established EU studies to critical approaches to European security, from Critical Data Studies to Governance Studies to Critical Geopolitics. By this, we offer a comprehensive, critical assessment of European digital sovereignty – the EU discourses and their scholarly analysis – and we regain analytical perspective on the relations between digital technology and politics and their effects on European security integration. Last, but not least, this pluralistic ethos allows us to explore the heuristic purchase of investigating how digital/sovereignty informs European security integration even when the term "digital sovereignty" is not rhetorically mobilised as such by European actors.

The rest of this article is organised in four parts, each building upon our own research and the conceptual and empirical insights of the Special Issue's contributions. In the first, we resituate the conceptual dyad digital/sovereignty at the intersection of Politics and STS, to showcase the value of those approaches that see knowledge infrastructures as crucial elements for statecraft. We then propose a taxonomy of three ways of approaching European digital sovereignty. In the third part, we characterise the emergence of an EU-formalised discourse on digital sovereignty with respect to a series of key policy developments not only at European and Member States' level, but also across the globe. In the last section, we offer an overview of the Special Issue's contributions showing their added value to understand unfolding dynamics of European security integration.

The puzzles of European digital sovereignty

The very idea of an EU digital sovereignty is puzzling. On the one hand, it conflates digital and sovereignty – which are two terms that orthodox EU studies are not used to conflating. On the other hand, it also conflates EU and sovereignty, whose nexus has been a mainstay in academic and political debates on European integration. Actually, as shown in the third part of the article, what is striking is the ease with which the state-centric sovereignty lexicon has been widely used in recent years by senior EU officials when addressing digital issues. Such a normalised or banalised use of the concept of sovereignty on the one hand, and the insistence of institutional discourses on the material, infrastructural and normative character of key digital technologies on the other hand, call for further research, and invite to do so from novel perspectives.

The concept of sovereignty lies at the heart of debates on the nature of European integration. Recently, conflicts of sovereignty have multiplied, not least in the fields of migration (Deleixhe and Duez, 2019), democracy and rule of law (Coman and Leconte, 2019). Moreover, as Brack *et al.* (2021) argue, these conflicts have been exacerbated and politicised. From this perspective, EU institutions' discourse on European digital sovereignty runs counter to key assumptions of EU Studies and International Relations. Across both disciplines, there is a scholarly consensus upon the fact that the EU is neither a state nor a nation-state. Several EU scholars have rather been claiming that, far from becoming a state, the EU is suffering from a growing systemic non-compliance problem, with Member States continuously not following EU Law. They mistrust EU authority and autonomy *vis-à-vis* the Member States, including in policy domains where the EU is supposed to have exclusive competence (Cremona, 2012, Börzel, 2021, p. 4).

Moreover, the concept of digital sovereignty sounds like an oxymoron (Pohle and Thiel, 2020). The deterministic approach to technology underpinning most International Relations pre-empts them from grasping how the seemingly immateriality and borderlessness of the digital may transform the existence, and exercise, of sovereignty (McCarthy, 2018). From this perspective, if there is already a tension between the concepts of European Union and territory, which is traditionally seen as a constitutive element of sovereignty, the digital can only contribute to a crisis of sovereignty as both an analytical and a political tool. Also, attempts to conceive of a European digital sovereignty may be hampered by the actual, and ever increasing, role of private actors and IT companies, in particular Big Tech such as Apple, Amazon, Google or Huawei (Farrand and Carrapico, this issue). It may seem strange or irrelevant to speak about EU digital sovereignty when it is no longer state authorities that rule the field but companies operating across the globe (van Dijck *et al.*, 2018).

Yet, thinking about European digital sovereignty gives us the occasion to go against the grain of oversimplified unitary approaches to sovereignty. We argue for going back to long-standing debates not only about the *meaning*, but also about the *practices* of sovereignty. Contrary to Ernst Haas who discarded the concept of sovereignty altogether in response to its unstable and fuzzy meaning – he once wrote, "I do not use the concept at all and see no need to" (Weber, 1994, p. 1) – we argue that sovereignty is a key *tool* of politics (Jackson, 1999 p. 431) that played a central role in the ordering of the modern world. To think of sovereignty in terms of practices means to focus on two interlinked elements. The first element is sovereignty as a *claim*. It is a normative premise or working hypothesis of modern political life, and it is actually this foundational character of sovereignty that explains the widespread ambiguity and numerous conflicts surrounding it (Avbelj, 2014, p. 346). According to Max Weber's (in Weber *et al.*, 2007 p. 77) classical definition, the state is a "human community that (successfully) *claims* the monopoly of the legitimate use of physical force within a given territory". Weber did not mean, by this, that an effective monopoly of the legitimate use of physical force has actually been observed. Rather, he only meant that the state is a political entity that consistently *claims* such a monopoly. Sovereignty is an unfulfilled political goal, insofar it is never truly absolute nor undisputed. As coined by Krasner (1999), it has always been a form of "organised hypocrisy". But it is a claim that comes with consequences since actors shape a given social order according to their normative worldviews. Furthermore, globalisation and the European integration processes have significantly undermined the absolute and

unitary conception of sovereignty, calling for further attention to how sovereign claims are denied, negotiated, reformulated in practice. European sovereignties are increasingly perceived as "shared business" (Keohane, 2002, p. 744). A wide range of metaphors are used to account for this transformation of sovereignty in the context of European integration (Brack *et al.*, 2019, p. 820) – sovereignty is described as "pooled" (Moravcsik, 1998, p. 67), "shared" (Wallace, 1999) or "plural" and "mixed" (Bellamy and Castiglione, 2005).

Second, sovereignty also implies a set of practices closely related to the production of knowledge about populations, territories and resources. As research focusing on the role of science and technology in society shows, this knowledge production needs infrastructures (Bowker and Star, 1999, Star, 1999). The development of sovereign political entities relies upon the creation of bureaucratic and centralised administrations and tools whose vocation is to quantify and, by doing so, to make a population legible and therefore governable (Desrosières, 1998, Scott, 1998). There is a strong historical connection between the development of tools such as statistics, demography and cartography, and the setting up of a tax administration to ensure the financing of wars or the setting up of police forces (Tilly, 1990, Elias, 2012). Despite his suggestion for a periodisation in which sovereignty would have been eroded by other forms of governance – discipline and then biopolitics – Foucault's works insist on the need to analyse the institutions and infrastructures that make possible to govern people and things (Foucault, 2009). Accepting here sovereignty as a placeholder for various and diverse forms of power, knowledge infrastructures are central in all Foucauldian-inspired studies of how actors think and – importantly – attempt to govern (Elden, 2007). In a sense, the current debate surrounding EU digital sovereignty may be just a new step in this long-term historical process. This seems to be the case because many knowledge infrastructures needed to govern populations, territories and resources – including in the domain of European security – nowadays rely on the processing of digital data, and the deployment of digital technologies (i.a. Jeandesboz, 2017, Amoore, 2020).

Despite the ubiquity of all things digital, grasping what digital actually means is a complex endeavour. As Peters (2016, p. 93) eloquently puts it, "the sweeping success of digital techniques has rendered the term a quintessentially twentieth-, not twenty-first-, century keyword". Still, we suggest embracing this challenge, rather than flatten our understanding of the digital into either digitalisation or the use of computing technologies. While the former refers to the "process of converting analogue information into the zeros and ones of binary code", the latter overlooks the history of computing, which predates digitalisation (Mayer-Schönberger and Cukier, 2013, p. 78). Without denying how digitalisation and computing are essential to any understanding of the digital, our approach invites to counter what Kirschenbaum (2004, p. 110) calls digital technologies' "illusion of immateriality". That is, a political imagination of the digital as devoid of any material, cognitive or political frictions, and – we should add – disembodied from historical dynamics of knowledge and governance. When we sit at the intersection of Political Science and STS, we can better see how the digital refers to, and re-signifies, different visions of government (Halpern, 2014, p. 12–27).

In line with our emphasis on the practices of sovereignty, we thus suggest approaching the digital through a focus on datafication and socio-material knowledge infrastructures. As we highlighted above, both are crucial technologies of modern statecraft, and allow for

the very possibility to practice sovereignty. While datafication processes predate the digital, the encounter between the two transforms states authorities worldviews and their action upon realities turned into digital databases (Amoore, 2013). Notably, the creation since the 1970s of national – and then European – digital databases equip state authorities with what Mann (1984, p. 15) has defined the "infrastructural power", that is "the capacity of the state to actually penetrate civil society, and to implement logistically political decisions through the realm". When it comes to digital sovereignty, this capacity (or lack thereof), ultimately relies, as Musiani (2022, p. 786) aptly notes, "on locally owned, controlled and operated innovation ecosystems, able to increase states' technical and economic independence and autonomy". Hence, it becomes important to explore how European security becomes reliant on datafication processes and knowledge infrastructures that are often controlled by private actors, either following the divestment of the public in domains previously considered at the core of sovereign action or following the adoption of commercial logics of "targeted governance" that presume access to commercial databases of financial or passenger transactions (Valverde and Mopas, 2004, Amoore and de Goede, 2008). In particular, it is the infrastructures that become "site[s] of multiple, overlapping, or nested forms of sovereignty, where domestic and transnational jurisdictions collide" in interaction or in parallel to statecraft (Easterling, 2014, p. 15).

More than any other policies, European security policies offer ideal case studies for analysing the shift towards new forms of data-driven power. Since its creation, the Area of Freedom, Security and Justice (AFSJ) has been a "dense socio-technical environment" (Bellanova and Duez, 2012, p. 110) filled with databases, information sharing systems and technologies for data collection and data management. European policing has become so digitalised that data collection and management has over time developed into a new policy domain dedicated to the management of large-scale IT systems with its own dedicated agency – euLISA (Jeandesboz, 2017, p. 5). For more than 20 years, the AFSJ has been questioning the relationship between sovereignty and the monopoly of force. It redefines the rationalities of security and contributes to the destabilisation of the Hobbesian's conceptual relation between sovereignty and the coercive state-based provision of security. The seemingly ubiquitous presence of Big Tech further contributes to such destabilisation (Srivastava, 2021, p. 2). For example, recent initiatives concerning the moderation of online terrorist content highlight how "European security decisions are co-produced at the intersection between public and private spheres" (Bellanova and de Goede, 2021, p. 15). Similar dynamics can be observed in Cybersecurity, a policy field that contains elements of both Justice and Home Affairs and Defence. Over the past decade, the EU has presented itself as being ideally positioned to address cyber insecurity, ranging from cyber-crime, such as ransomware, to cyber-attacks on critical information infrastructures (EP *et al.*, 2013). Given the borderless nature of cyber insecurity, the EU argues that Member States alone do not have the right instruments to tackle this problem and has offered to coordinate the collection of information about cyber threats, provide situational analyses based on its capacity to have a bird's eye-view, and coordinate the action of Member States through the creation of new specialised bodies, such as ENISA and EC3. Although it does not replace Member States' initiatives, it is presenting itself as the solution to Member States' limitations (Carrapico and Barrinha, 2017).

EU-promoted technology-driven security practices are a socio-technical fix to overcome the main drawback of European security policies. Indeed, European integration has had a limited impact on the re-distribution of regalian powers (Duez, 2019), with the EU still lacking the prerogative and tools of the sovereign, i.e. police services, customs, criminal courts and military. Through the development and deployment of digital technologies, the EU could formulate an answer to a challenging question: how to be a security actor without controlling the traditional means of security policies? The creation of European law enforcement bodies – Europol and more recently the European Public Prosecutor's Office – as well as the upgrade of Frontex into a European Border and Coast Guard Agency do not suffice to meet the ambition of a genuine "Security Union" (EC, 2020a). Therefore, in addition to these institutional innovations, the EU has chosen to invest in the building of new security digital infrastructures to reconcile its ambitions on security with the Member States' desire to keep their sovereign prerogatives unaltered (cf. also Bellanova and Glouftsios, this issue). In a more classical EU studies wording, faced with the risk of another "capability-expectations gap" (Hill, 1993), the EU has supported and amplified ongoing changes in how security policies are enacted. Building on the growing importance given to the exchange and processing of information in law enforcement, to the detriment of more traditional forms of coercion, the EU posited itself as an information broker as well as a policy entrepreneur promoting new security technologies and strategies (Jeandesboz, 2017). By so doing, in a long-term perspective, the EU is challenging nothing less than the Weberian vision of political authority.

Our broader approach to the digital offers a vantage point to better understand the unfolding EU emphasis on digital sovereignty. Bratton (2015, p. 20–21) notes that the entanglements of sovereignty and the digital – or software, in his words – are not novel, "but rather that both are now mutually contingent and that the work of software at a global scale itself produces unfamiliar sorts of sovereignties". In this sense, focusing on digital sovereignty offers us the much-needed occasion to study how digital and sovereignty reshape each other. By foregrounding the evolving role of datafication and knowledge infrastructures, we can emphasise ongoing transformations of European sovereignty. This feeds, notably, into those security literatures that take in account how the EU and other institutions have been, and are, taking seriously the transformative effects of digital technologies. Notably, these include works focusing on the creation of an Area of Freedom, Security and Justice as part of a longer historical transformation of statecraft (Walters and Haahr, 2005, Broeders and Dijstelbloem, 2016), the growing landscape of EU databases asserting digital worldview and "hardwiring" cooperation (Andersson, 2016, Jeandesboz, 2022) or EU cybersecurity ambitions (Carrapico and Barrinha, 2017, Dunn Cavelty, 2018, Christou, 2019). Despite their diverse conceptual approaches – ranging from governmentality to STS, from collective securitisation to new institutionalism – these works show the value of focusing on what we call digital/sovereignty not in terms of radical innovation, but with attention to specific changes to the politics and technologies shaping European integration.

Towards a taxonomy for thinking European digital sovereignty

The concept of sovereignty has had rather stable theoretical foundations, dating as far as the mid-sixteenth century. But these foundations have been challenged by

European integration. Drawing from the convergent work of Bellamy (2017), Avbelj (2014) and Deleixhe and Duez (2019) on the interaction between sovereignty and European integration, we finetune and propose a three-fold taxonomy of the different approaches to sovereignty in the European context. Here, we explicitly draw on the work carried out by one of us with Deleixhe (Deleixhe and Duez, 2019, p. 924–926), to propose a taxonomy that classifies existing scholarly approaches as *traditional*, *post-sovereignist* and *post-traditional*. Such a distinction can help us to better grasp the variety of digital sovereignty claims, their conceptual background as well as the worldview underpinning them.

The traditional perspective on sovereignty highlights the identification of the sovereign with the authority to end conflicts among subjects for the ultimate sake of maintaining peace within the polity (Bodin, 1955[1576]; Hobbes, 1996[1651]). This perspective is thus unitarian, in the sense that it purports the existence of a supreme authority that cannot be challenged by others. This perspective also understands sovereignty as indivisible, as sharing such ultimate authority would risk creating competing sites of power (Prokhovnik, 2008, p. 40–41). It involves the creation of a territorial polity and an institutional apparatus, i.e. a state, to defend its independence externally from other sovereign polities and to fend off internal challenges to its authority. This ideational creation is expected to resist the passing of time and even major historical upheavals. The post-sovereignist perspective, on the other hand, emerged as a critique of the traditional view of sovereignty. For post-sovereignists, we have left behind the Westphalian period, and its projection of the traditional sovereignty ideas. According to this second perspective, the Westphalian world may have never existed, and sovereignty would amount to a powerful political myth. In fact, post-sovereignists' critique is mostly derived from the empirical observation that Nation-states are not the only relevant political units anymore, and that historical, technological, environmental and ideological factors continuously affects power relations and our own understanding and experience of what matters for the polity (Castells, 1996, Sassen, 1996, Beck, 2018). Hence, from a post-sovereignist perspective, the notion of sovereignty shall be replaced by a conception of governing that goes beyond *the* state, *the* territory or *the* supreme authority. A third perspective on sovereignty – the post-traditional approach – demarcates itself from the other two by refusing linear readings of sovereignty. Instead of understanding it as immutable or radically discontinued, this perspective approaches sovereignty as dynamic and transformative (Prokhovnik, 2007). This means that sovereignty keeps changing across history, responding to various challenges by adjusting itself both in ideational and practical terms without fading into irrelevance. This perspective moves away from grand theories of sovereignty, and rather favours a more situated analysis of how sovereignty changes at critical, historical junctions (see: Keohane and Hoffmann, 1991; Habermas, 1996; Rosanvallon, 2000).

If we use this tripartite classification, we can identify three diverse foci of research on European digital sovereignty. First, a traditionalist approach to EU digital sovereignty would, in a zero-sum game perspective, pay attention to the distribution of power between the Member States and the EU, or to the competition between the EU and the US or China. More importantly, it would look for or, in a more normative stance, *call for* elements pointing at the building of a territorialised European supreme authority. On the contrary, in a post-sovereignist approach, one would consider EU digital sovereignty as not being sovereignty at all. It would be something in-between a mere

buzzword and a name given to something that might be completely new, but that should still be defined. Finally, analysed through the lens of a post-traditionalist approach, EU digital sovereignty would indeed be a kind of sovereignty that would not break entirely out of the traditional mould of sovereignty, but would nevertheless disaggregate and reassemble some of its constitutive elements in relation to the evolving and diverse nature of the digital. Due to its attentiveness to the constant evolution of the concept, this is also the approach that can better cater for the continuous re-articulation of sovereignty and the digital, or what we have called digital/sovereignty.

With a few nuances, all the articles collected in this special issue fall under the post-traditionalist approach to sovereignty. On the one hand, they do not see in the current evolutions a general process, both conscious and deliberate, aiming at giving shape to a European state, territorialised and claiming absolute authority for itself, against Member States. On the other hand, all the articles underline the performative and transformative effects of the European discourse on digital sovereignty. Even though these effects are seen as more or less important depending on the point of view of the authors and/or the case studies selected, they all highlight the consequences of EU discourses and sovereignty practices (both claims and knowledge infrastructures) in terms of redefinition of EU politics. All the articles show that the narrative of European digital sovereignty is not just a slogan lacking in political content or transformative power. Quite the contrary, they show that this narrative gives shape to a new European security imaginary (Oliveira Martins, Lidén and Jumbert, this issue) that is accompanied by actual transformations in the way sovereignty is conceived.

In the following section, we show that this new European security imaginary articulates two different but complementary issues. The first concerns sovereignty *over* the digital, meaning the fight for control *over* digital tools and infrastructures. This first issue reflects the concern for the EU's dependence on non-European technological companies, a dependence that should be overcame by strengthening the EU's capacities in terms of technological innovation, but also by developing specifically European critical digital infrastructures. The second issue concerns sovereignty *through* digital technology. It reflects the growing desire of Europeans to develop digital tools for the governance and the security of spaces, people and objects. Here, the EU's objective is rather to interconnect and make digital tools developed at the national and EU level work together, in particular by promoting standardisation, interoperability and dissemination of EU norms and values.

Overview of EU digital sovereignty conceptualisations

The emergence of a rhetoric about digital sovereignty, and its underlying concerns, may be new in the context of EU institutions and policies, but it has been part of a much wider discussion whose origins go back to the United States' digital hegemony and surveillance programmes of the late 1990s (Thumfart, 2022). Interest in the concept can be traced back to two interrelated debates: (1) the challenges brought about by the rapidly developing cyberspace and accompanying infrastructure to US capacity to control digital activities and communities and (2) the ability of the State to access personal data for security purposes and without the need for individual consent in the aftermath of 9/11. Countries such as China and Russia quickly followed suit by questioning US hegemony in this

field and by attempting to assert their control over national infrastructures and data (Budnitsky and Jia, 2018, Couture and Toupin, 2019). China developed a concept of digital sovereignty that is intimately connected to national security, and which promotes the need to treat digital sovereignty as equivalent to a territorial one (Jiang, 2010). The Russian debate emerged a few years later out of concern over internal political upheaval, as well as increased fears over US surveillance, and resulted in increased State regulation of the Internet, including content and free speech regulation, and of the actors involved in digital infrastructure (Budnitsky and Jia, 2018). Comparatively, the EU and its Member States constitute a more recent addition to the wider digital sovereignty debate. Starting with concerns expressed first by France and, later, by Germany, the EU's engagement with the concept of digital sovereignty has been the result of Member States uploading their understandings of the role of the digital world in the context of the International System. If China and Russia have developed a territorial approach to digital sovereignty, shaped by the perception that the digital world is fraught with US cultural and political hegemonic ideas that must be resisted, the EU and Member States have moved in the direction of a *critical cooperation approach* (Cattaruzza *et al.*, 2016).

At Member State level, digital sovereignty discussions emerged in France, in the mid to late 2000s, out of concern for data privacy and loss of economic competitiveness (Gheham, 2017). The gradual awareness within French society that citizens' personal data were being accessed, transferred to, and processed by US-affiliated companies gave rise to feelings of loss of control over that data and promoted an important mediatic debate based on the folowing three main elements: (1) whether citizens should have a say over the treatment of their data; (2) whether private companies, namely foreign ones, should be trusted with personal data and (3) whether any personal data and consumer information should be transferred beyond national and EU borders (Bellanger, 2014). This perceived loss of control also stemmed from economic anxieties over market dominance by large foreign corporations such as Google, Amazon, Facebook, Apple and Microsoft (also popularised as GAFAM), which were understood as reducing the industrial and economic development of France, transferring added value abroad and limiting the capacity for innovation (Floridi, 2020). Responses to these concerns resulted in a greater political willingness to adopt more interventionist and localised solutions. It was the case of the Hadopi Law (2009), which aimed at regulating the exchange of copyrighted material online in order to protect cultural heritage, as well as the LOPPSI 2 law (2011), which expanded law enforcement authorities' capacity to address cyber-crime, namely child sexual exploitation and identity theft (Cattaruzza *et al.*, 2016). Attempts to create local solutions also included projects aimed at competing with US cloud computing technology, such as Andromede (2009), Cloudwatt (2012) and Numergy (2012) (Gheham, 2017).

Similar concerns also emerged in Germany, although the 2013 Snowden revelations – of the widespread global surveillance activities carried out by US intelligence services – reoriented the debate towards a security approach. In addition to the issues previously highlighted in the French debate of the State's capacity to regulate, of individuals' digital self-determination, and of economic and technological competitiveness, Germany also focused on the importance of protecting national IT infrastructure from external interference, developing counter-surveillance technologies, reducing the transfer of data beyond EU borders and decreasing technological dependency on non-EU

countries by encouraging the creation of national IT products (Pohle, 2020). Rather than marking a simple re-territorialisation of digital regulation and practices, however, French and German initiatives shifted the digital sovereignty debate to the EU level. Both claimed that the only way to achieve real sovereignty was not just by acting nationally but mainly by working together at the European level. In 2013, the French Minister of Culture, Catherine Morin-Desailly, argued that if the EU did not act to protect its digital sovereignty, soon France and the EU would find themselves as a "colony of the digital world" (Morin-Desailly, 2013). The same year, the German Minister of the Interior, Thomas de Maizière, commented that acting through the EU was key to achieving the country's security and economic strategy, including digital sovereignty (Steiger *et al.*, 2017). And a few months later, faced with the need to address the US mass surveillance leak, his successor, Hans-Peter Friedrich, called explicitly for the development of a European infrastructure with a view to achieving digital sovereignty. The Snowden revelations, therefore, accelerate the process of Europeanisation of the French and German concepts of digital sovereignty (Traynor, 2015, De Hert and Thumfart, 2018).

Throughout the Juncker Commission term (2014–2019), it was already possible to observe a nascent EU discussion that, not only reflected the concerns expressed by France and Germany (economic, data protection, EU values and security), but also reacted to a number of external events and processes such as the Snowden revelations and foreign interference with democratic elections and referenda. Linked to economic and technological competitiveness, the EU Commissioner for the Digital Economy and Society, Günther Oettinger, promoted the concept as part of a European Single Digital market project, which would be capable of facing the US, China, Russia and India: "The European Commission has responded to the digital revolution with its Digital Single Market Strategy […] The objective is to build a Digital Union, which can ensure Europe's digital sovereignty and competitiveness in a lasting fashion" (Oettinger, 2016, p. 1). The concern with citizens' data protection and privacy also became visible with the EU Court of Justice (CJEU)'s decision to invalidate the transatlantic data protection agreement with the US, known as the Safe Harbour Agreement. The decision was brought about by an EU citizen's complaint that the transfer of personal data by Facebook from its Irish subsidiary to US local servers was infringing on his fundamental rights, given that the US did not offer an adequate level of protection for personal data (Court of Justice of the European, 2015). Although not explicitly mentioned, the 2015 CJEU decision relates to digital sovereignty in the sense that it recognises the importance of protecting EU citizens' data from foreign surveillance, and hints at the idea that other countries might not share the same individual rights-based EU values.

This concern with EU values as directly associated with digital sovereignty was another element that emerged during this period, as clearly articulated by Viviane Reding's (2016, p. 10) speech: "we can use our European sovereignty to set the gold standards of the digital age in the domain of data protection and beyond. This […] will shape the world we hand over to our children. I want it to be a world where European values and decisions still matter". The security concern appeared by association with the three other types of concern mentioned above. More specifically, it was presented as a pre-requisite for the protection of the digital economy, the competitiveness of the industry, the safeguard of the physical and digital infrastructure, and the preservation of EU values. As phrased by the Commission's Science and Knowledge Service (EC, 2020b), "cybersecurity is a

pillar of the European sovereignty for the future". Key initiatives in this area have focused on securing critical information infrastructures, ensuring cyber resilience, regulating online illegal activity and promoting EU-produced/hosted digital products, such as Gaia-X (Christakis, 2020).

If the Juncker Commission term was characterised by the emergence of interrelated concerns which were often addressed in isolation, the arrival of the von der Leyen Commission marked a shift towards a more structured and strategic thinking about digital security, which positions this concept at the heart of the EU integration project. In her vision for the 2019–2024 Commission, von der Leyen (2019, p. 4) claimed that "Europe must lead the transition to a […] new digital world, by achieving technological and digital sovereignty." This idea has been re-stated by the other main EU institutions, which is indicative that the concept has now entered mainstream EU discourse. Digital sovereignty is the strategy that will allow the EU to achieve economic and industrial development, to protect EU citizens' data, to guarantee EU fundamental rights, and to secure physical and information critical infrastructures: "Europe must bolster digital sovereignty to effectively respond to future challenges, guarantee livelihoods and ensure the security of its citizens" (German Presidency of the Council of the European Union, 2020). In fact, digital sovereignty has become synonym with the protection of the EU integration project itself (European Council, 2020, European Council, 2021, Michel, 2021).

The rhetoric on EU digital sovereignty, however, has remained fairly vague, and has often been produced and replicated by different EU actors with little coordination as to the direction of this emerging discourse (Roberts *et al.*, 2021). Furthermore, there have been limited attempts at defining what the EU understands by the concept of digital sovereignty (Barrinha and Christou, this issue), what it wishes to achieve through its usage (Lambach and Monsees, this issue), and how it proposes to do so on the basis of its current legal and political toolbox (Celeste, 2021). Current EU policy documents and speeches that make reference to the concept frame it as an attempt to regain control over the digital field and to develop international leadership capacity as a reaction to five interrelated concerns: (1) the EU's growing awareness of its dependence on non-EU digital infrastructures, services and content providers whose interests may not align themselves with EU ones (Madiega, 2020); (2) A lack of control over such infrastructures, services and content providers, which manifests itself in a reduced say over EU citizens' data and its protection (Pohle, 2020, Celeste, 2021), and in a diminished capacity to enforce national and EU legislation (Moerel and Timmers, 2021); (3) The loss of competitiveness, and reduced revenue, over the past few years of EU-based technological companies and their shrinking international market presence (European Commission, 2020a); (4) The impact of this loss of competitiveness on the EU's capacity to develop trustworthy technology that fully embodies EU norms and values, and the consequent repercussions on the development of the Common Market (European Commission, 2020b) and (5) the EU's level of vulnerability to a wide range of cyber threats, including denial of service attacks, data breaches, ransomware and mis/disinformation targeting democratic institutions and public services (Moerel and Timmers, 2021).

What we have been observing, therefore, is a *rhetorical performativity* (Couture and Toupin, 2019) that contrasts the geopolitical, security and economic challenges that the EU is facing in the twenty-first century with the vision it has for its future as an integration project. More specifically, digital sovereignty foregrounds the importance of an EU

approach that is not only normative or legislative, but actually infrastructural and geopolitical (Lambach and Monsees, this issue, Bellanova and Glouftsios, this issue), that is, able to set up socio-legal and material standards and instruments that would assert the EU's role in an increasingly digital world (Barrinha and Christou, this issue, Lambach and Monsees, this issue). What emerges from the EU's current discourse is an understanding of the digital not as a disembodied realm, but an all too material site of global politics in which economy, security and values are at stake. Furthermore, the formulation of these concerns, their discursive framing as endangering the health of the EU as an integration project, and the proposed solutions transversal to all policy fields and to all Member States, allow it to introduce an innovative element in its discourse, that of a supranational organisation claiming sovereignty for itself. This bold move reflects, above all, a vision of what kind of international actor, including what kind of security actor, the EU wishes to be: one that may not be able to project force in the traditional sense, but which is able to coordinate Member State action in order to protect the EU and its citizens from the security threats posed by cyberespionage, cyber-attacks, cyber-crime and the over-dependence on foreign digital services and technology. Even when no formal claim to digital sovereignty is made, we can observe a certain convergence towards this practice of sovereignty across other key security policy domains, such as AFSJ (Bellanova and Glouftsios, this issue). It would be important to mention that although the EU's discourse on digital sovereignty is for the moment much more focused on cybersecurity elements, it has also started to emerge in other more traditional areas of security such as Justice and Home Affairs (Oliveira Martins, Lidén and Jumbert, this issue) and Defence (Csernatoni, this issue). In fact, given the transversality of the EU cybersecurity policy, it is likely that references to digital sovereignty will become ever more prominent in an increasing number of fields. Finally, the EU's rhetoric on digital sovereignty invites us to further unpack how the EU is re-articulating sovereign power and digital technologies in a post-traditional approach to sovereignty and how it is reshaping European security integration by leveraging on a traditional notion of modern statecraft (Bellamy, 2017) and by evoking a novel socio-technical imaginary (Jasanoff & Kim, 2015). The last section of this editorial presents how the articles in the Special Issue contribute towards this unpacking.

Overview of the contributions and the way forward

The Special Issue is organised in two parts – conceptual approaches and case studies. In the first section, the Special Issue puts forward diverse conceptual approaches engaging with digital sovereignty and its implications for European security integration. In the first article, Barrinha and Christou offer a wider contextualisation of the discussion on EU digital and technological sovereignty, as they ask what the practical effects are of the EU taking ownership of a traditionally statist concept such as "sovereignty" and applying it to cyberspace. They problematise the concept of technological sovereignty in the context of the EU's fluid cyber ecosystem, and assess the EU's claim to sovereignty by exploring the conceptual delineation, legitimacy and policy operationalisation. The central implications of this form of sovereignty claim for furthering the EU's international leadership in cybersecurity are also explored. Conversely, Lambach and Monsees suggest deconstructing the concept of digital sovereignty by analysing the different assumptions, patterns of justification and threat-images that constitute the geopolitical imaginaries at

the basis of the EU digital sovereignty discourse and of the projection of the EU as a global player. In particular, these authors explore how specific projects such as 5G, Gaia-X and the semi-conductor industry are being legitimised by framing them in digital sovereignty terms. In the third article of the Special Issue, Csernatoni explores the evolution of the EU's rhetoric on digital sovereignty as it is currently being used to frame the EU defence technological and industrial base. She suggests unpacking the scaled-up EU rhetoric to understand the way the meaning of digital and technological sovereignty is not fixed but rather articulated via hegemonic interventions across a number of connected fields. The article makes the case that the "travelling" and the "stretching" of the concept of digital sovereignty is likely to have profound implications for the future of European integration by fostering a more unified security imaginary of the EU as an independent global security actor.

In the case study section, the Special Issue exemplifies our understanding of how digital sovereignty plays out in practice across diverse security-related domains, ranging from more established to emerging ones. Calderaro and Blumfelde analyse how the EU is positioning itself in the geo-politics of cyber by looking at EU initiatives advancing Artificial Intelligence and Quantum Computing standards. The article analyses how the EU is adopting protectionist strategies to ensure the safety of EU citizens' data, as part of its aim to develop digital sovereignty, as well as how it is presenting itself in the context of the current technological race, which will have important repercussions for EU Foreign Security. Farrand and Carrapico explore the role of the private sector within the discourse and practices of EU digital sovereignty. More specifically, these authors highlight the transformative power of digital sovereignty discourse regarding EU priorities, values, norms and threats, by reflecting on trust relations in the context of public–private cooperation in cybersecurity. They argue that the EU's strategy to achieve digital sovereignty has resulted in a re-thinking of these partnerships, with the non-EU private sector being framed as a security threat from whom digital sovereignty must be secured. Bellanova and Glouftsios focus on the interoperability of JHA databases to unpack how the socio-material reorganisation of databases informs European security politics. The article does so by exploring the operational and epistemic anxieties informing interoperability, as well as the socio-technical mechanisms that define how public authorities (such as law enforcement, border and migration ones) and EU agencies can access information across all EU centralised databases. In doing so, they insist on the importance of catering for the "political role of infrastructures" to better grasp the ongoing re-articulation of digital/sovereignty. In the final case study, Jumbert, Liden and Oliveira Martins study EU external border governance as a site for politics of digital sovereignty by exploring the use of digital databases and systems including EURODAC, the shared Biometric Matching System, and the West Africa Police Information System. The authors analyse the dynamics taking place within the digitalisation of EU borders: expansion, interoperability and deterritorialisation and reflect on how they relate to the digital/sovereignty.

As a whole, the Special Issue highlights that the future of the notion of digital sovereignty is still uncertain. Yet, it calls for further analysis. Digital sovereignty might be just another buzzword or hype, as the EU has known so many in the past. As such, it could be doomed to disappear, gradually replaced by others, equally fashionable and ephemeral terms. However, whatever the political future of the concept of digital sovereignty,

the general focus of the Special Issue on digital/sovereignty, as well as all the contributions gathered, show that there are ongoing major dynamics that need to be studied and better understood. These dynamics concern the EU's attempt to develop and control digital security infrastructures (sovereignty *over* the digital), as well as the use of digital technologies for European security governance (sovereignty *through* the digital). Beyond the vague and often confusing use by EU officials of the heavily politically charged concept of sovereignty, all the articles make the case for engaging in an academic conversation at the intersection of Political Science, European Studies, Law and Science and Technology Studies. This Special Issue of *European Security* aims to be a stepping-stone in that direction, offering a pluralistic, transdisciplinary and empirically informed approach to the relationship between the digital and European security.

Additional information

Authors are listed in alphabetical order, and have contributed equally to the article. They thank the Editors for their support and guidance, as well as the anonymous reviewers for their constructive feedback on this article and the other contributions to the Special Issue.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The research study of Rocco Bellanova and Denis Duez' was funded by the Université Saint-Louis – Bruxelles in the framework of the preparation of the Centre of Excellence Jean Monnet EUNMUTE, to be funded by the European Union under the Erasmus+Programme [620597-EPP-1-2020-1-UK-EPPJMO-CHAIR]. The research study of Helena Carrapico was co-funded by Northumbria University and the European Union under the Erasmus+Programme [Jean Monnet Chair Grant Agreement No 824135]. The views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

ORCID

Rocco Bellanova http://orcid.org/0000-0001-6222-6636
Denis Duez http://orcid.org/0000-0002-5751-3531

References

Amoore, L., 2013. *The politics of possibility. Risk and security beyond probability*. Durham: Duke University Press.
Amoore, L., 2020. *Cloud ethics*. Durham: Duke University Press.
Amoore, L., and De Goede, M., 2008. *Risk and the war on terror*. London: Routledge.
Andersson, R., 2016. Hardwiring the frontier? The politics of security technology in Europe's 'fight against illegal migration'. *Security dialogue*, 47, 22–39.
Avbelj, M., 2014. Theorizing sovereignty and European integration. *Ratio juris*, 27, 344–363.
Barrinha, A., and Christou, G., 2022. Speaking sovereignty: the EU in the Cyber Domain. *European Security*, 31 (3), 356–376.

Beck, U., 2018. *What is globalization? Cambridge*. Cambridge: Polity Press.
Bellamy, R., 2017. A European republic of sovereign states: sovereignty, republicanism and the European Union. *European journal of political theory*, 16, 188–209.
Bellamy, R., and Castiglione, D., 2005. Building the Union: the nature of sovereignty in the political architecture of Europe. *In*: D. Karmis and W. Norman, eds. *Theories of federalism: a reader* (pp. 293–310). New York: Palgrave Macmillan US.
Bellanger, P., 2014. *La souveraineté numérique*. Paris: Stock.
Bellanova, R., and De Goede, M., 2021. Co-producing security: platform content moderation and European security integration. *JCMS: journal of common market studies*. https://doi.org/10.1111/jcms.13306
Bellanova, R., and Duez, D., 2012. A different view on the 'making' of European security: the EU passenger name record system as a socio-technical assemblage. *European foreign affairs review*, 17, 109–124.
Bellanova, R., and Glouftsios, G., 2022. Formatting European security integration through database interoperability. *European Security*, 31 (3), 454–474.
Bigo, D., 2014. The (in)securitization practices of the three universes of EU border control: military/navy – border guards/police – database analysts. *Security dialogue*, 45, 209–225.
Bodin, J., 1955[1576]. *Six books of the commonwealth*. Oxford: Oxford University Press.
Borrell, J. 2020. Why European strategic autonomy matters. European External Action Service. *HR/VP blog* [Online]. Available from: https://eeas.europa.eu/headquarters/headquarters-homepage/89865/why-european-strategic-autonomy-matters_en.
Börzel, T., 2021. *Why noncompliance. The politics of law in the European Union*. Ithaca: Cornell University Press.
Bossong, R., and Carrapico, H.2016. *EU borders and shifting internal security – technology, externalization and accountability*. Heidelberg: Springer.
Bowker, G.C., and Star, S.L., 1999. *Sorting things out*. Cambridge, MA: MIT Press.
Brack, N., Coman, R., and Crespy, A., 2019. Unpacking old and new conflicts of sovereignty in the European polity. *Journal of European integration*, 41, 817–832.
Brack, N., Coman, R., and Crespy, A., 2021. *Understanding conflicts of sovereignty in the EU*. London: Routledge.
Bratton, B., 2015. *The stack. On software and sovereignty*. Cambridge, MA: MIT Press.
Broeders, D., and Dijstelbloem, H., 2016. The datafication of mobility and migration management. *In*: I. Van Der Ploeg and J. Pridmore, eds. *Digitizing identities* (pp. 242–260). London: Routledge.
Budnitsky, S., and Jia, L., 2018. Branding internet sovereignty: digital media and the Chinese–Russian cyberalliance. *European journal of cultural studies*, 21, 594–613.
Calcara, A., Csernatoni, R., and Lavallée, C.2020. *Emerging security technologies and EU governance*. London: Routledge.
Calderaro, A., and Blumfelde, 2022. Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security*, 31 (3), 415–434.
Carrapico, H., and Barrinha, A., 2017. The EU as a coherent (cyber)security actor? *JCMS: journal of common market studies*, 55, 1254–1272.
Castells, M., 1996. *The rise of the network society*. Oxford: Blackwell.
Cattaruzza, A., *et al.* Sovereignty in cyberspace: balkanization or democratization. 2016 International Conference on Cyber Conflict (CyCon U.S.), 2016/10// 2016. 1–9.
Celeste, E., 2021. Digital sovereignty in the EU: challenges and future perspectives. *In*: F. Fabbrini, E. Celeste, and J. Quinn, eds. *Data protection beyond borders*. Oxford: Hart.
Christakis, T., 2020. *'European digital sovereignty': successfully navigating between the 'Brussels Effect' and Europe's quest for strategic autonomy*. Rochester, NY: Social Science Research Network.
Christou, G., 2016. *Cybersecurity in the European Union*. New York: Palgrave.
Christou, G., 2019. The collective securitisation of cyberspace in the European Union. *West European politics*, 42, 278–301.

Coman, R., and Leconte, C., 2019. Contesting EU authority in the name of European identity: the new clothes of the sovereignty discourse in Central Europe. *Journal of European integration*, 41, 855–870.
Court Of Justice Of The European, U. 2015. Case C-362/14, Schrems v Data Protection Commissioner.
Couture, S., and Toupin, S., 2019. What does the notion of "sovereignty" mean when referring to the digital? *New media & society*, 21, 2305–2322.
Cremona, M.2012. *Compliance and the enforcement of EU Law*. Oxford: Oxford University Press.
Csernatoni, R., 2022. The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European Security*, 31 (3), 395–414.
De Goede, M., 2012. The SWIFT affair and the global politics of European security. *Journal of common market studies*, 50, 214–230.
De Hert, P., and Thumfart, J., 2018. The Microsoft Ireland case and the cyberspace sovereignty trilemma. *Brussels privacy Hub working paper*, 4, 1–27.
Deleixhe, M., and Duez, D., 2019. The new European border and coast guard agency: pooling sovereignty or giving it up? *Journal of European integration*, 41, 921–936.
Desrosières, A., 1998. *The politics of large numbers*. Cambridge, MA: Harvard University Press.
Duez, D., 2019. De l'État à l'Union. Pour une sociologie historique de la sécurité intérieure européenne. *Politique Européenne*, 65, 30–61.
Dunn Cavelty, M., 2018. Europe's cyber-power. *European politics and society*, 19, 304–320.
Easterling, K., 2014. *Extrastatecraft. The power of infrastructure space*. London: Verso.
EC, 2020a. *Communication […] on the EU Security Union Strategy*. Brussels: European Commission.
EC, 2020b. *Cybersecurity – our digital anchor – a European perspective*. Brussels: EU Science Hub - European Commission.
Elden, S., 2007. Governmentality, calculation, territory. *Environment and planning D: society and space*, 25, 562–580.
Elias, N., 2012. *On the process of civilisation: sociogenetic and psychogenetic investigations*. Dublin: UCD Press.
Ep, Council, Eesc & Cotr, 2013. *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace*. Brussels: High Representative of the EU for Foreign Affairs and Security Policy.
European Council. 2020. Shaping Europe's Digital Future- Council Conclusions- 8711/20.
European Council. 2021. European Council Meeting Conclusions- EUCO 17/21.
Farrand, B., and Carrapico, H., 2022. Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, 31 (3), 435–453.
Floridi, L., 2020. The fight for digital sovereignty: what it is, and why it matters, especially for the EU. *Philosophy & technology*, 33, 369–378.
Foucault, M., 2009. *Security, territory, population*. New York: Picador/Palgrave Macmillan.
German Presidency of the Council of the European Union. 2020. Expanding the EU's digital sovereignty.
Gheham, F. 2017. Digital sovereignty – steps towards a new system of Internet Governance. Fondation pour l'Innovation Politique.
Habermas, J., 1996. *Between facts and norms*. Cambridge: Polity Press.
Halpern, O., 2014. *Beautiful data. A history of vision and reason since 1945*. Durham: Duke University Press.
Hill, C., 1993. The capability-expectations gap, or conceptualizing Europe's international role. *JCMS: journal of common market studies*, 31, 305–328.
Hobbes, T., 1996[1651]. *Leviathan or the matter, forme and power of a common wealth ecclesiasticall and civil*. Oxford: Oxford University Press.
Hobbs, C. (Ed.). 2020. *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*. Essay Collection. European Council on Foreign Relations.
Jackson, R., 1999. Sovereignty in World Politics: a Glance at the Conceptual and Historical Landscape. *Political Studies*, 47, 431–456.
Jasanoff, S., and Kim, S.H.2015. *Dreamscapes of modernity. Sociotechnical imaginaries and the fabrication of power*. Chicago, IL: University of Chicago Press.
Jeandesboz, J., 2017. European border policing: EUROSUR, knowledge, calculation. *Global crime*, 18, 256–285.

Jeandesboz, J., 2022. European Union information systems for border and migration enforcement: trajectories, programmatics, and uses. *In*: G. Hudson and I. Atak, eds. *Migration, security, and resistance* (pp. 47–65). London: Routledge.
Jiang, M., 2010. Authoritarian informationalism: China's approach to internet sovereignty. *SAIS review of international affairs*, 30, 71–89.
Kaunert, C., and Léonard, S., 2019. The collective securitisation of terrorism in the European Union. *West European politics*, 42, 261–277.
Keohane, R.O., 2002. Ironies of sovereignty: the European Union and the United States. *JCMS: journal of common market studies*, 40, 743–765.
Keohane, R.O., and Hoffmann, S., 1991. *The new European community*. Boulder: Westview Press.
Kirschenbaum, M., 2004. Extreme inscription. *TEXT technology*, 13, 91–125.
Krasner, S.D., 1999. *Sovereignty: organized hypocrisy*. Princeton, NJ: Princeton University Press.
Madiega, T., 2020. *Digital sovereignty for Europe* (No. PE 651.992). European Parliamentary Research Service, European Parliament.
Mann, M., 1984. The autonomous power of the state: its origins, mechanisms and results. *European journal of sociology / archives européennes de sociologie / europäisches archiv für soziologie*, 25, 185–213.
Mayer-Schönberger, V., and Cukier, K., 2013. *Big data*. Boston, MA: Eamon Dolan.
Mccarthy, D., 2018. Introduction. Technology in world politics. *In*: D. Mccarthy, ed. *Technology and world politics* (pp. 1–22). London: Routledge.
Michel, C. 2021. Digital sovereignty is central to European strategic autonomy – Speech by President Charles Michel at "Masters of digital 2021" online event.
Moerel, L., and Timmers, P., 2021. *Reflections on digital sovereignty*. Rochester, NY: Social Science Research Network.
Mogherini, F., 2016. *Shared vision, common action: a stronger Europe*. Brussels: High Representative of the Union for Foreign Affairs and Security Policy and Vice-President of the European Commission.
Monsees, L., and Lambach, D., 2022. Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, 31 (3), 377–394.
Moravcsik, A., 1998. *The choice for Europe. Social purpose and state power from Messina to Maastricht*. London: Routledge.
Morin-Desailly, C. 2013. L'Union européenne, colonie du monde numérique? Paris, Commission des Affaires Europeennes, Senat.
Musiani, F., 2022. Infrastructuring digital sovereignty. *Information, communication & society*, 25, 785–800.
Oettinger, G. 2016. Speech: EU Commissioner Oettinger at WSBI innovation conference.
Olviveira Martins, B., Liden, K., and Jumbert, M.G., 2022. Border security and the digitalization of sovereignty: insights from EU borderwork. *European security*, 31 (3), 475–494.
Peters, B., 2016. Digital. *In*: B. Peters, ed. *Digital keywords. A vocabulary of information society & culture* (pp. 93–108). Princeton: Princeton University Press.
Pohle, J., 2020. *Digital sovereignty. A new key concept of digital policy in Germany and Europe*. Berlin: Konrad-Adenauer-Stiftung.
Pohle, J., and Thiel, T., 2020. Digital sovereignty. *Internet policy review*, 9, 1–19.
Prokhovnik, R., 2007. *Sovereignties: contemporary theory and practice*. New York: Palgrave Macmillan.
Prokhovnik, R., 2008. *Sovereignty. History and theory*. Exeter: Imprint Academic.
Reding, V., 2016. Digital sovereignty: Europe at a crossroads. *European investment bank institute*.
Roberts, H., *et al.*, 2021. Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet policy review*, 10. https://doi.org/10.14763/2021.3.1575
Rosanvallon, P., 2000. *La Démocratie inachevée: histoire de la souveraineté du peuple en France*. Paris: Gallimard.
Sassen, S., 1996. *Losing control?: sovereignty in the age of globalization*. New York: Columbia University Press.
Scott, J.C., 1998. *Seeing like a state*. New Haven, CT: Yale University Press.

Srivastava, S., 2021. Algorithmic governance and the international politics of Big Tech. *Perspectives on politics*, 1–12. https://doi.org/10.1017/S1537592721003145
Star, S.L., 1999. The ethnography of infrastructure. *American behavioral scientist*, 43, 377–391.
Steiger, S., Schünemann, W.J., and Dimmroth, K., 2017. Outrage without consequences? Post-Snowden discourses and governmental practice in Germany. *Media and communication*, 5, 7–16.
Thumfart, J., 2022. The norm development of digital sovereignty between China, Russia, the EU and the US: from the late 1990s to the Covid-crisis 2020/21 as catalytic event. *In*: D. Hallinan, R. Leenes, and P. De Hert, eds. *CPDP 2021: enforcing rights in a changing world* (pp. 1–44). London: Hart Publishing.
Tilly, C., 1990. *Coercion, capital, and European states, AD 990–1990*. Cambridge, MA: Blackwell.
Traynor, I., 2015. EU unveils plans to set up digital single market for online firms. *The Guardian*, 2015/05/06/T14:44:39.000Z.
Valverde, M., and Mopas, M.S., 2004. Insecurity and the dream of targeted governance. *In*: W. Larner and W. Walters, eds. *Global governmentality* (pp. 1–44). New York: Routledge.
Van Dijck, J., Poell, T., and De Waal, M., 2018. *The platform society*. Oxford: Oxford University Press.
Von Der Leyen, U., 2019. *A Europe that strives for more: my agenda for Europe*. Luxembourg: Publications office of the European Union.
Wallace, W., 1999. The sharing of sovereignty: the European Paradox. *Political studies*, 47, 503–521.
Walters, W., and Haahr, J.H., 2005. *Governing Europe*. Oxon: Routledge.
Weber, C., 1994. *Simulating sovereignty: intervention, the state and symbolic exchange*. Cambridge: Cambridge University Press.
Weber, M., Gerth, H., and Wright, M.C.2007. *From Max Weber: essays in sociology*. London: Routledge.