European Security

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

Speaking sovereignty: the EU in the cyber domain

André Barrinha & G. Christou

To cite this article: André Barrinha & G. Christou (2022) Speaking sovereignty: the EU in the cyber domain, European Security, 31:3, 356-376, DOI: 10.1080/09662839.2022.2102895

To link to this article: https://doi.org/10.1080/09662839.2022.2102895

Published online: 09 Sep 2022.

EUROPEAN SECURITY
2022, VOL. 31, NO. 3, 356–376
https://doi.org/10.1080/09662839.2022.2102895

Routledge
Taylor & Francis Group

Speaking sovereignty: the EU in the cyber domain

André Barrinha[a] and G. Christou[b]

[a]Politics, Languages and International Studies, University of Bath, Bath, UK; [b]Politics and International Studies, University of Warwick, Coventry, UK

ABSTRACT

The EU's revised Cybersecurity Strategy (2020) has been constructed in the context of increasing geopolitical tension and within a dynamically evolving technological environment. The onset of new technologies has brought with it new opportunities but also perceived risks and threats in cyberspace, to which the EU has sought to elicit a more comprehensive approach underpinned by a move to become more "technologically sovereign". We seek in this article to critically unpack what such claims to technological sovereignty mean for the EU in the cyber domain and what the practical implications are of the EU taking ownership of and performing sovereignty. More specifically, in seeking to conceptually unpack technological sovereignty in its internal and external manifestations, we show how its articulation, legitimisation and operationalisation has implications and consequences for the EU's identity and action in the cyber domain.

ARTICLE HISTORY
Received 23 November 2021
Accepted 14 July 2022

KEYWORDS
Technological sovereignty; digital sovereignty; cybersecurity; othering; European Union; European security

Introduction

The EU has in recent years sought to elicit a comprehensive set of responses to the perceived risks and threats emanating from cyberspace. Those responses build on already established guiding concepts and signifiers such as resilience, deterrence, and defence, as well as on a complex array of policy and operational tools and mechanisms, now packaged in a sovereigntist discourse, that is visible in its revised Cybersecurity Strategy (European Commission and High Representative of the Union 2020, pp. 4–12). The achievement of technological sovereignty, as noted by several scholars, has frequently been projected by the EU as a key goal alongside the promotion of strategic autonomy; even if the debate has lacked differentiation, nuance and conceptual clarity in relation to what this implies for the EU's ability to govern and lead when it comes to cybersecurity and emerging technologies (Timmers 2019), but also more broadly in terms of its common foreign and security and other external policies (Youngs 2021).

We seek in this article to critically analyse the meaning and implications of the EU's willingness to be more assertive in the cyber domain within the broader framework of technological sovereignty (Mueller 2020, Thumfart 2021). We argue that only through critically

CONTACT André Barrinha a.barrinha@bath.ac.uk

interrogating, problematising and unpacking such a concept can we begin to build a deeper understanding of the central implications for enhancing the EU's cyber resilience and shaping the EU's international identity and leadership in cybersecurity. More specifically, we will assert that in embracing a sovereignty discourse, the EU is legitimising a specific worldview that may not always be compatible with its own ambitions of an open and free cyberspace; and that may willingly or unwillingly construct othering dynamics with allies and competitors alike. We will, in this context, ask how the EU constructs its idea of sovereignty in the cyber domain, and how that translates into specific policies, actions, and ethical stances. In particular:

- What does it mean to be technologically sovereign in cyberspace and how can we provide conceptual markers to further our understanding of the EU as a technologically sovereign actor?
- What are the EU's discursive understandings of technological sovereignty and how does it construct and justify its move to being technologically sovereign?
- What are the consequences of "claiming" and performing technological sovereignty?

Asking such questions will first allow us to embed our theoretical discussion and argument in the debates on technological (and digital) sovereignty. This will provide conceptual markers for understanding the EU as "technologically sovereign" entity. Second, we will seek to establish how in articulating a particular type of sovereignty imbued with certain norms, ethics and values, the EU aligns itself with like-minded states but also pits itself against Others – with implications for its ability to interact in the broader cyber domain. This way, we seek to contribute to the still emerging literature on European technological sovereignty (Couture and Toupin 2019, Burwell and Propp 2020, Christakis 2020, Hobbs 2020, Komaitis 2021) by offering both a conceptual framework to further study the issue (including beyond the cyber-domain), and by problematising the implications of saying "sovereignty" in this domain.

This article is broken down into the following sections to articulate the above argument. The second section provides a discussion of sovereignty as a discourse of power and suggests an analytical framework that allows us to address our core questions and unpack the EU's technological sovereignty move. The third section systematically assesses the EU's claim to technological sovereignty through three analytical steps: conceptual delineation; legitimacy; and policy operationalisation. This section also explores the implications of this for the EU's external leadership and international actorness in cybersecurity, with the final section providing reflection on the EU technological sovereignty and the challenges the EU faces in moving from constructing and claiming to performing technological sovereignty.

Sovereignty in the digital sphere

As perceptively remarked by Gammeltoft-Hansen and Adler-Nissen (2008, p. 3) few "words have begotten so much dispute, confusion, and opaqueness as that of sovereignty". Although it is seen as one of the fundamental institutions of international relations, and a crucial pillar of international law, its meaning has been contested throughout history. Ultimately, sovereignty is a term that has been used in the West

since the Middle Ages to legitimise power, particularly in moments of crisis (Werner and De Wilde 2001, p. 287). Internally, it is a positive concept, representing the supreme power of deciding, governing, and commanding; internationally, it has a negative meaning, indicating the absence of a higher authority (Christakis 2020, p. 5). More broadly, sovereignty brings with it a specific episteme, a "particular way of knowing, representing, and ordering the social and political world" (Walker 2008, p. 23), a world "in which the division of mankind into distinct peoples is regarded as an inescapable and perhaps even desirable condition" (Bartelson 2008, p. 45). As argued by Robert Elliot Mills (2014, p. 113), sovereignty's "principal function" is differentiation, be it from other sovereigns or from its opposite, what the author calls the anti-sovereign (in relation to piracy). Based on Charland's idea of constitutive rhetoric, but also on Laclau and Mouffe's work on antagonism, Mills (2014, p. 116) highlights how this differentiation is an inherent part of any rhetorical move. In that sense, sovereignty "constitutes international relations differentially" and it is not possible to say "sovereignty" without activating those differentiating dynamics. Although this can often be associated with territorialisation claims – for Thumfart (2021, p. 4) "[i]n practice, sovereignty is primarily attached to territory" – by focusing on discourse and its effects, it becomes possible to go beyond that discussion; in that, territory is not an essential claim of sovereignty, but one frequently used to justify its two key dynamics – (internal) authority and (external) autonomy (in a context of inter-dependence). Fundamentally, a claim to sovereignty is a claim to power.

While accepting that our analysis starts from that assumption – that sovereignty elicits a specific worldview – its focus is not on what sovereignty "is" or "ought" to be;[1] but rather on how it is articulated and constituted politically. In that sense, we follow authors such as Walker (2008), and Werner and De Wilde (2001), in understanding sovereignty as a form of performative political discourse (Werner and De Wilde 2001, p. 287). Therefore, our approach sits closer to what the introduction to this special issue defines as a post-traditionalist approach to sovereignty (see Bellanova *et al.*, this issue). But if one accepts, as we do, that sovereignty is a type of discourse with clear performative features, how does one go from words to deeds? We propose that a successful sovereignty claim contemplates three steps: conceptual delineation, legitimisation, and policy operationalisation.

Conceptual delineation. A claim to sovereignty is never independent of its context. As a fundamentally contested concept, it needs to be located. This is the case in general claims to sovereignty, but even most important when it comes to sectorial claims, such as is the case regarding food sovereignty or, as discussed below, technological sovereignty. "Becoming" sovereign involves uttering that over which one claims ultimate authority. This involves, using Gammeltoft-Hansen and Adler-Nissen's (2008) typology (albeit not their definitions), which consists of a vertical and horizontal dimension. Vertically, it delineates who has the ultimate political authority over an issue or territory. Horizontally, it defines the scope of areas or territories over which it claims to command that authority. This first step is then, at least in theory, followed by legitimation claims.

Legitimation. The most fundamental aspect of a sovereignty discourse is that by claiming it one is "providing a distinctive discursive register" (Walker 2008, p. 26) to an audience (or multiple audiences): domestically, the claim to ultimate authority and externally, a claim to equality (among peers). The legitimation of "being" sovereign, also entails the legitimation of the sovereign's use of its power (Werner and De Wilde 2001, p. 287).

Policy operationalisation. In that regard, "being" sovereign and "doing" sovereignty are closely linked. The concept "has real effects on social and political practice" (Walker 2008, p. 26), starting with how resources are allocated, and policies are ordered, inter-linked and prioritised. This operationalisation of sovereignty corresponds to the effective materialisation of the audience's approval.

This model can help us make sense of different sovereignty claims, including those related to technology, as explored in what remains of this article.

Technological sovereignty in cyberspace

The notion of technological sovereignty goes back to the late 1960s, with references found in official documents in Canada and Australia, both related to the need to empower technological innovation nationally (Couture and Toupin 2019, p. 2310). In the cyber-domain, China and Russia have both advocated the idea of information sovereignty at least since the 1990s.

The concept is usually associated with ideas of "independence, control and autonomy" (Couture and Toupin 2019, p. 2317). This can be linked to calls for innovation and technological development, or have a focus on security, be it of the state or that of the individual (usually associated with privacy concerns). Although the concept remains fundamentally state-centric, for some, technology has exacerbated the claims of other actors to the point we are now witnessing "a shift from the collective—the state as its typical expression—to the individual" (Couture and Toupin 2019, p. 2317). In 1996, John Perry Barlow talked about cyber-sovereignty, where cyberspace (and its users) were free from the shackles of states. This idea of cyber-exceptionalism, in which "the digital realm is qualitatively distinct from the analogue world" (Pohle and Thiel 2020, p. 4), has been frequently advocated in the US, particularly in Silicon Valley, where it has often been associated with ideas of cyber libertarianism. For Milton Mueller (2020, p. 780), "[t]erritoriality and authority are sundered in cyberspace for reasons deeply embedded in its technical architecture and current configuration".

Another international practice that pushes against a state-led sovereign cyber-domain is that of multi-stakeholderism in internet governance. This is defined by "the principles of openness, inclusion, bottom-up collaboration and consensual decision-making" (Pohle and Thiel 2020, p. 4) between different actors, including states, but also, civil society, the private sector and academia. The early 2000s saw an open challenge against this model, particularly from authoritarian regimes, but not exclusively, as the EU was for a time also interested in a more multilateral form of internet governance. The fundamental problem was the US-centred nature of the institutions called to regulate the internet, particularly the Internet Corporation for Assigned Names and Numbers (ICANN), created in 1998 as a registered organisation in the US Department of Commerce, under US law (Carr 2015). The 2001 US PATRIOT Act further added to the suspicion regarding the US hegemony over cyberspace. However, the focus was mostly on data sovereignty, and the debate was "foremost restricted to expert circles" due to yet limited dependence on digital technologies, particularly the internet (Thumfart 2021, p. 5).

A decade later, the scepticism against US technological hegemony in cyberspace was to find another episode in Edward Snowden's leaks of the National Security Agency (NSA) global surveillance initiatives. In Brazil, steps were taken to accelerate

the construction of an undersea cable linking South America to Europe, so that they were not dependent on US infrastructure to route their data, and in Europe, calls for data sovereignty were uttered by Germany and France. In the case of the latter, the Snowden disclosures served to reinforce the image in France of Europe's "lack of control and independence over the evolution of digital networks" (Couture and Toupin 2019, p. 2312, Bellanger 2012). In 2010, China's State Council Information Office had circulated a white paper discussing the idea of internet sovereignty, which was actively promoted in subsequent international fora, including China's World Internet Conference in Wuzhen (Mueller, 2020, p. 787). China, and other states, have consistently advocated for a multilateralisation of internet governance, giving a greater role to the International Telecommunication Union (ITU) and critically, placing states at the forefront of decision-making in this domain. Not by coincidence, Houlin Zhao, a Chinese engineer, was elected ITU Secretary-General in 2014.

In the USA, the term never gained traction, at least in a positive sense, as it retained its connotation with an authoritarian understanding of sovereignty (Pohle and Thiel 2020, p. 11). In recent years, the debate has been framed within the dispute between the US and China – the so-called Cold War 2.0 – but also as part of the discussion around the emergence of Big Tech as international players, both through their social media influence and economic wealth (Christakis 2020, p. 6).

As Milton Mueller (2020, p. 780) points out,

> [i]t is indicative of the changing times that the first papers to raise the issue of cyber-sovereignty were animated not by attempts to apply traditional forms of state sovereignty to cyberspace but by the claim that cyberspace itself was its own sovereign space.

In that sense, there may be merit in Tim Wu's (1997) claim that the absence of sovereign discussions on cyberspace was mostly due to the lack of states' interest. States have not only decided to pay more attention to the matter, turning it into an issue of significant geopolitical interest (Barrinha and Renard 2020). They are actively attempting to address the sovereignty gap identified by Lucas Kello (2018, p. 190), in which states understand that: they "are no longer the sole or even the main objects of concern of other states in the protection of national security"; they cannot "take for granted their ability to protect national security against all relevant threats"; and that, they "are not the sole masters, even of interactions among themselves".

At this stage, it is important to highlight that although there is a potential difference between technological and digital sovereignty – with the former being more encompassing than the latter, including the material components that enable the digital to exist – there is little in the literature, or indeed in EU documents, separating both. These are both overlapping, but ultimately, unsettled concepts. As argued by Johannes Thumfart, it

> is crucial to keep in mind that the developing concept of digital sovereignty and related terms do not have a specific fixed meaning (yet), but rather, their meaning changes with the traditions they come from, the contexts in which they are used and the power-relations inherent to those contexts. (2021, p. 5)

This is a discussion that reflects "the power struggles over internet governance amongst the world's major rival military powers" (Mueller 2020, p. 786) but fundamentally, this is an exercise in imposing "a familiar order" – that of state sovereignty – "upon a new

sociotechnical system" (Mueller 2020, p. 784). Therefore, it is essential to subject it "to ideo-historical contextualization and discourse analysis" (Thumfart 2021, p. 5).

As is the case regarding the use of the concept more generally, talking about sovereignty in the digital context also has a "rhetorical performativity", in that it enables the assertion of authority over a certain realm and it sets different forms of opposition to certain hegemonies, be it the "US", "China", or "corporate hegemony" (Couture and Topin 2019, p. 2317). When it comes to the analysis of the EU's technological sovereignty discourse, we propose an analytical model that combines the above-identified steps – conceptual delineation, legitimisation, and policy operationalisation – with the authority and autonomy dynamics, as presented in Table 1.

Methodologically, this model qualifies a sovereign claim, but it does not quantify it, nor does it offer a definite answer on whether a specific actor "is" or "is not" sovereign. As indicated earlier, our assumption is that any credible claim to sovereignty will generate political effects, regardless of the underlying capacity or intention of those that claim it. In that sense, this model tries to understand what sovereignty "does". Our assumption is that any claim to sovereignty – be it sectoral or generic – goes through equivalent processes of delimitation, legitimisation and operationalisation, both internally and externally. Therefore, conceptually, the model is not exclusive to the technological domain, but it was delineated with the European Union in mind, particularly in the potential identification of the horizontal (as an actor without exclusive competences across all policy areas), and vertical (as an actor that regularly negotiates its existence with other sovereign entities – its member states) dimensions. What follows is an application of the model to the EU's activities and policies in cyberspace. This will be done through a discourse analysis of the EU's strategic and key policy documents from 2013 – when the first cyber security strategy was published – until 2021. In each of the documents analysed, we asked: *how does the EU define itself as sovereign*? *how does it legitimise itself as sovereign*? and *how does it operationalise its sovereign claim*? By allowing us to analyse the EU's claims[2] during this period and identify its temporal continuities and discontinuities, this approach will help us understand "the layer of reality where meaning is produced and distributed" (Wæver 2009, p. 165) without necessarily committing to a reified construction of the EU's actorness in this domain.

The construction of the EU technological/digital sovereign

Strategic autonomy in the EU's security and defence has been visible for some time and was made prominent in the EU's Global Strategy in June 2016 (European External Action

Table 1. Sovereignty - An Analytical Framework

Steps/Dynamics	(Internal) authority	(External) autonomy
Conceptual delineation	Who are the actors entitled to be sovereign (vertical)? What are the areas/policies identified as part of the conceptual delineation (horizontal)?	How is the conceptual delineation of sovereignty distinct from those of other actors?
Legitimation	How is the claim to authority justified within the context of current powers/competences?	How is the claim to equality/autonomy justified?
Policy operationalisation	What are the policies and resources that have to be operationalised in order to ensure the success of the sovereign claim?	What partnerships, principles, processes, and/or norms must be established to ensure the autonomy of the sovereign?

Service, 2017). Even though the idea, in practice, existed prior to this in, for example, the General Data Protection Regulation, the language of technological or digital sovereignty is a recent addition to the EU lexicon (see Bellanova *et al.*, this issue) developed in a specific geopolitical context to address issues of security, technological innovation and economic competitiveness in Information and Communication Technology (ICT), as well as to support a functioning European democratic society in an era of digital transition. The concepts of technological and digital sovereignty did not appear at all in the EU's 2013 Cybersecurity Strategy (European Commission and High Representative 2013) or 2017 (*de facto*) revision of it, although the latter did emphasise "building greater resilience and *strategic autonomy*, boosting capabilities in terms of technology and skills, as well as helping to build a strong single market" (European Commission and High Representative 2017, p. 2, *our emphasis*). It was only in the EU's cybersecurity strategy of December 2020 that the term "technological sovereignty" appeared more explicitly, as part of three areas of action which included: (1) resilience, *technological sovereignty* and leadership, (2) building operational capacity to prevent, deter and respond, and (3) advancing a global and open cyberspace (European Commission and High Representative 2020, p. 4, *our emphasis*).

The use of the term "sovereignty" has intensified since 2019, particularly with Ursula von der Leyen's "geopolitical Commission" that has called for the EU to "have mastery of key technologies" and "infrastructure fit for the future with common standards, gigabit networks, and secure clouds of both current and next generations" (European Commission 2019). Digital sovereignty has also been constructed as an ambitious strategy by the President of the European Council, Charles Michel, who has argued that it includes "a truly digital single market, defining our own rules, making autonomous technological choices and developing our own digital solutions" (European Council, 2020a). Indeed, EU leaders have stressed "the need to enhance the EU's digital sovereignty in a self-determined and open manner" (European Council and Council of the EU, Video Conference of the members of the European Council, 25–25 March 2021) – a sentiment echoed by EU member states, and in particular France and Germany, who have been at the forefront, for example, of EU cloud initiatives such as GAIA-X based on the principle of sovereignty-by-design (Moerel and Timmers 2021, p. 6; for detail on GAIS-X, see Monsees and Lambach, this issue).

Conceptual delineation

(a) Who are the actors entitled to be sovereign (vertical)?

Constructing and projecting technological sovereignty is a collective enterprise driven by increasing risks and threats to Europe that have been exacerbated by the COVID-19 pandemic. Here, numerous Council Conclusions (European Council, 2020a; 2020b) have reiterated the importance of secure and resilient digital transformation, with Members of the European Council on 25 March 2021 underlining "the need to enhance Europe's digital sovereignty in a self-determined and open manner by building on its strengths and reducing its weaknesses and through smart and selective action, preserving open markets and global cooperation" (European Council 2021, p. 3). These conclusions were also meaningful in combining different aspects of cybersecurity, in a clear indication of the EU's willingness to have a more encompassing view of the field.

Of course, this also raises questions of not just formal political authority in relation to EU Member States and EU institutions but also of those actors that are exercising – or are deemed to be exercising – digital sovereignty beyond the "state". Here, there is a tension between those projecting corporate authority and the ambitions of EU Member States and the EU institutions – in particular the geopolitical Commission but also the European Parliament – in constructing and implementing digital sovereignty. The COVID-19 pandemic, in particular, has seen leading tech companies rather than democratically elected governments (and legitimately elected institutions) acting as private governments that are making choices that impact on society (Moerel and Timmers 2021, p. 5). As pointed out by Madiega (2020, p. 3), in the context of COVID-19, "technological choices made by Apple and Google have frustrated the ability of some Member States to design their own contact-tracing solutions … and fuelled the quest for digital sovereignty".

There is a fine balance to be had between the coherence of the EU's approach to cybersecurity in this context (Carrapico and Barrinha 2017) and the engagement with other actors, particularly member states and companies (on the latter, see Farrand and Carrapico, this issue). If the last few years showed an increasing assertiveness on the part of the EU in this field, and a willingness to further concentrate decision-making and the allocation of resources, the discourse of sovereignty serves to existentially justify that tendency. In that regard, when it comes to EU cybersecurity, it is not a matter of who is entitled to be sovereign, but of what transfers of power and resources take place and in which direction when sovereignty is claimed. This is very much linked with the delineation of the areas and policies associated with technological sovereignty in cyberspace. Thus, the EU has promoted technological sovereignty to be achieved through open strategic autonomy; securing safe and resilient tech supply and infrastructure through a multi-stakeholder approach to ensure an open, free Internet and democratic society. EU leaders have also recently "stressed the need to enhance the EU's digital sovereignty in a self-determined and open manner" (European Council and Council of the EU, Video Conference of the members of the European Council, 25–25 March 2021).

(b) What are the areas/policies identified as part of the conceptual delineation (horizontal)?

The European Council's Strategic Agenda 2019–2024 (European Council and Council of the European Union, 2019) highlights the need for the EU to act autonomously in international affairs. Such strategic autonomy, from an EU perspective, is not simply narrowly focused on security and defence, even though this is where it predominantly evolved. Indeed, as the EU's High Representative, Josep Borrell, has highlighted, strategic autonomy is a process of political survival, and as such, applies to other sectors considered to be strategically important for the EU (Borell 2020). As noted by Moerel and Timmers (2020, p. 7) the "new sovereignty thinking is not limited to digital policy, and … encompasses an almost kaleidoscope range of initiatives and measures" that relate to health, energy, finance, foreign direct investment, supply chains, among others. To this end then, "the underlying logic behind strategic autonomy has started to increasingly encompass discussions about technological protectionism and capacity building in new domains related to digitalization, data, space, energy and new and emerging technologies" (Csernatoni 2021). This in turn, begs questions of how we understand technological

sovereignty within the EU's broader strategic sovereignty (Hobbs 2020, Fiott 2021) and autonomy ambitions; and in terms of the connections between strategic sectors but also the scope of the EU's technological and digital objectives.

In this context, we can observe that the EU's technological sovereignty remit cuts across multiple pillars, including a human-centric approach to technology development, a fair and competitive digital economy, an open, democratic and sustainable digital society and the EU as a global standard setter in the digital field (Adonis 2020). These pillars, in turn, are visible across various inter-related and cross-cutting dimensions, which include security and defence (research and technological capacity and capability (see Csernatoni, this issue)), investment in digital/technological research and innovation, CIP and Resilience/security of supply, and regulatory activism, protection and projection (including data sovereignty) (Csernatoni 2021). Thus, and important in relation to the EU's cyber assertiveness, invoking digital or technological sovereignty has implications for how the EU seeks to engage, project and influence internally, but also externally in relation to cybersecurity, in particular through its strategic partnerships and at multilateral and regional levels, as we discuss in more detail next.

(c) How is the conceptual delineation of sovereignty distinct from those of other actors?

EU leaders have "stressed the need to enhance the EU's digital sovereignty in a self-determined and open manner" (European Council and Council of the EU 2021a). In the post-COVID-19 environment,

> the EU aims to protect and reinforce its digital sovereignty and leadership in strategic international digital value chains as key elements to ensure strategic autonomy in the digital area, whilst also promoting common EU values and respecting fundamental freedoms, including data protection and privacy, safety and security. (European Council and Council of the EU 2021b)

It is clear that the EU's discourse on technological sovereignty is predicated on differentiating it from Others, public and private, that are seen to contravene the interests, norms and values that the EU is seeking to protect and project internally and externally. To this end, EU articulation of technological sovereignty differs most starkly (but not only) – normatively and ethically – from that supported by authoritarian regimes for the purpose of control, repression, suppression and conditioning of citizens. This places "states" front and centre of decision-making domestically and multilaterally to ensure power can be centralised and political authority maximised within and for a given political territory. Here, narrations of network or information sovereignty and indeed a sovereign internet are not in support of global, open and free cyberspace in the liberal sense, but rather in the sense of ensuring the ordering and bordering of the digital world in the name of preserving a certain national identity, culture and security. Such states then, threaten EU values and interests through pursing practices underpinned by broader strategies of sovereign control and (territorial) stability and indeed technological expansion and export (for example, 5G infrastructure) the security of which, is perceived as a risk and threat. As stated above, however, the EU is not only constructing its technological or digital sovereignty against states considered to be "different" but also from companies – predominantly Chinese and from the US – that prioritise practices such as data

appropriation and monetisation, threaten EU citizens control over their personal data and that constrain "the growth of EU high-technology companies and the ability of national and EU rule-makers to enforce their laws" (Madiega, 2020, p. 1).

It is somewhat paradoxical that a supranational body such as the EU actively promotes a statist concept – sovereignty – in order to address a set of issues that fundamentally challenge one of the core principles of the concept (territoriality). It does so by attempting to insulate rather than isolate itself from the global cyberspace ecosystem. For the EU, the concept is firmly connected to ideas of cybersecurity and resilience in an open and free cyberspace, but also more broadly in the digitalisation of Europe. There are of course questions raised by this approach – and in particular on how far the EU can navigate the construction of its own brand of technological sovereignty to avoid accusations of protectionism and a fortress digital Europe that excludes and is closed rather than inclusive, engaging and open (Bauer and Erixon 2020, Christakis 2020, Ilves and Osula 2020, March and Schieferdecker 2021). The conceptual delimitation of sovereignty clearly involves both openness and control in cyberspace, two concepts that do not necessarily or naturally complement each other in practice.

Legitimising sovereignty

(a) How is the claim to authority justified within the context of current powers/competences?

The justification for increasing EU competence and autonomy through technological sovereignty and strategic autonomy, as alluded to, relates to geopolitical and geo-economic rivalries as well as an increasing risk and threat landscape exacerbated by the COVID-19 pandemic.

To this end, what is at stake has been made clear across the EU institutional milieu. While there was recognition (and indeed policies, such as that on privacy, data protection and anti-trust levies) under the Juncker Commission "that Europe had to protect its values, interests, and citizens in a digital space that was gradually becoming a geopolitical and geo-economic battleground" (Hobbs 2020, p. 91), it was the Commission under the leadership of Ursula von der Leyen that made digital policy a political and politicised priority and the achievement of technological sovereignty a necessity in critical "digital" issue areas.[3] Member States, through the European Council, have also called – in the context of challenges faced – for the EU to "go further in developing a competitive, secure, inclusive and ethical digital economy with world-class connectivity" with emphasis on "access to, sharing of and use of data, on data security and on Artificial Intelligence, in an environment of trust" (European Council 2019). In addition to this, the Commission and the European Parliament (European Parliament 2019) have highlighted the increasing risks and challenges that stem from those actors that do not comply with European protocols and rules – and indeed do not reflect the same values or apply the same security standards – leaving European citizens, society and industry vulnerable to manipulation, exploitation and attack (Madiega, 2020).

(b) How is the claim to equality/autonomy justified?

It is clear then that there has been a discursive recognition and agreement that only a collective response underpinned by technological sovereignty and the vehicle of strategic

autonomy will sufficiently mitigate shared risks and threats emanating from increased digitalisation but also ensure a more sustainable, secure and resilient technological ecosystem for the future. It is also clear that the case for autonomy and sovereignty has been justified through what is at stake for the EU and its member states across society, economy and the political realm, in particular in relation to preserving a safe, secure, stable and resilient European, democratic, way of life.

This threat landscape has been exacerbated by the COVID-19 pandemic, which exposed particular vulnerabilities in Europe relating to the security of online platforms, locational data and privacy issues when using contact-tracing apps and the proliferation of disinformation on social media (Burtwell and Propp 2020, p. 2). Indeed, as asserted by Hobbs (2020, p. 93)

> *Europeans' complete dependence on technology to not only sustain the economy as millions worked from home during lockdown, but to even combat the virus itself, overnight made Europe's digital transformation a question of existential importance. Rising tensions and digital decoupling between China and the US during the pandemic added an additional element of urgency, with Europe no longer able to simply spectate but instead forced to pick a lane or define its own.*

The need to enhance Europe's digital sovereignty – and to accelerate efforts given the COVID-19 pandemic – was emphasised in the Conclusions of the European Council of March 2021 (European Council 2021). The pandemic thus created more urgency among EU policy-makers and within EU Member States on how to achieve digital transition and transformation in safe and secure manner to ensure resilience, innovation and growth. As confirmed in the European Council Conclusions of 1–2 October 2020 "[t]he COVID-19 pandemic has further underlined the need to accelerate the digital transition in Europe" so that we can "safeguard our values, fundamental rights and security, and be socially balanced. Such a human-centred approach will increase the attractiveness of the EU model. (2020a, p. 4)The defence and promotion of the EU's values through technology is very much salient here as part of its move to legitimise its sovereignty moves.

There is a broad consensus within the EU that "[d]igitalisation has the potential to provide solutions for many of the challenges Europe and Europeans are facing" (European Council 2021) and that sovereignty, EU leadership and strategic autonomy in the digital sphere are essential if the aims of the EU's Digital Strategy are to be realised. In this context, certain scholars have called for the further embedding of the concept of sovereignty within the EU Treaties (Moerel and Timmers 2021, p. 30, Wolff *et al*. 2021) to ensure there is coherence in the way in which the EU manages its "sovereignty" across different digital dimensions and sectors; a move that could further contribute to enhancing the legitimacy of the EU's sovereignty claims.

Operationalising sovereignty

(a) What are the policies and resources that have to be operationalised in order to ensure the success of the sovereign claim?

The EU has mobilised several policies, initiatives and instruments (see Figure 1) in the name of constructing and protecting its digital sovereignty and achieving technological strategic autonomy. It has also pledged to increase its financial resource to meet its digital

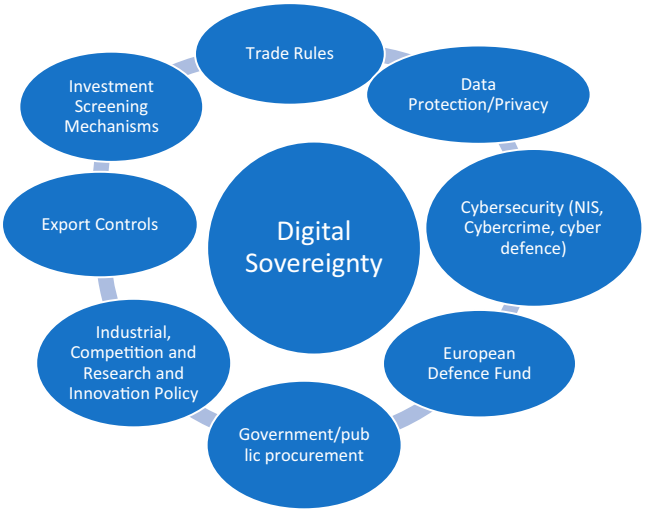

Figure 1. EU Digital Sovereignty Policy Tools. Source: Adopted from European Political Strategy Centre (2019), 15.

goals.[4] For example, 8 billion Euros has been allocated to developing the next generation of supercomputers (European Commission 2020, State of the Union Address) to be made in Europe, for Europe – and 2 billion Euros of EU funding committed to developing a European cloud infrastructure and services, with the aim of additional funds of between 2 and 4 billion invested by EU Member States and industry to establish "EU-wide common, interoperable data spaces in strategic sectors" (European Commission 2020, A European Strategy for Data). Furthermore, EU defence and research and development initiatives have been agreed to support the competitiveness of the European Defence Technological and Industrial base for some time. The European Commission's European Defence Fund (allocated 8 billion Euros in the MFF 2021-2027) and sub-programmes such as the Preparatory Action on Defence Research and the European Defence Industrial Programme "are intended to financially empower the EU's autonomy in defense technology and industry and its research and innovation capacity in future-oriented and disruptive defense technologies" (Csernatoni 2021; see also Csernatoni, this issue).

Cybersecurity appears as one of the multiple areas that congregates around the idea of digital sovereignty, even if, in practice, it cuts across most of them, including AI and 5G. The EU has taken a number of (interdependent) approaches to perform and achieving strategic autonomy in cyberspace, including a risk management-based regulatory approach, such as in the case of GDPR or the NIS Directive (being updated at the time of writing), cultivating strategic partners and partnerships (with states or companies that are like-minded) and regional (e.g. through ASEAN Regional Forum) and global level cooperation (e.g. at the UN) to find solutions in the common interest (Moeler and Timmers 2021, p. 19–20). All have implications for the EU reducing its dependencies and becoming a global leader in the digital sphere, and all are employed and prioritised to differing degrees by the EU in performing its "technological sovereignty".

In recent years, the EU has also repackaged some of its cyber-related initiatives as directly contributing to that ambition. This is most evident in the case of the 2020

Cybersecurity Strategy, where the Cybersecurity Industrial, Technology and Research Competence Centre and Network of Coordination Centres (CCCN) are identified as potentially playing "a key role in … developing the EU's technological sovereignty in cybersecurity" (European Commission and High Representative 2020, p. 11). The CCCN was initially proposed in the 2017 Communication Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. In the document, there is no reference to sovereignty regarding this new centre, only that "[t]his network and its Centre would stimulate development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level" (European Commission and High Representative of the Union for Foreign Affairs and Security Policy 2017, p. 9).

While the EU's 2020 Cybersecurity Strategy for the Digital Decade (2020) refers to technological sovereignty as one of its key domains, the term is not unpacked in any substance throughout the document. However, when one reads the communication on the European Commission's website, the connection between the document and the concept of technological sovereignty becomes more tightly linked. There one can read that the "The strategy describes how the EU can harness and strengthen all its tools and resources to be technologically sovereign". It further adds that the "EU's technological sovereignty needs to be founded on the resilience of all connected services and products" and therefore, the four cybercommunities identified in the document – internal market, law enforcement, diplomacy and defence – "need to work more closely towards a shared awareness of threats … [and] be ready to respond collectively when an attack materialises". This will enable the EU to be "greater than the sum of its parts".[5] The repackaging of previously proposed policies or documents along the lines of technological sovereignty supports the argument regarding the aggregating features of the concept, but also shows how the three elements – conceptual delimitation, legitimation and policy operationalisation – are fluid and interactive. The operationalisation of a policy can be justified along sovereign lines, but when doing so, it is also contributing to redefine those lines and reinforce the claims to legitimacy from those that purpose it.

This operationalisation of the EU's sovereignty sits side by side with the will of its member states. In this sense, moves towards constructing and constituting the EU's sovereignty narratives and indeed implementing policies operationalised under the sovereignty claim, is reliant on effective vertical coherence if it is to result in a collective strengthening of the EU and its subsequent leadership and assertiveness in the cyber field. For example, in terms of public procurement and decisions on components for 5G networks – this very much remains a member state competence and despite clear guidelines and a risk-based approach (which includes the exclusion of high-risk vendors) being provided by the European Commission through its 5G Toolbox on such procurement decisions – there is still variation in Member State treatment of the purchase of 5G from Huawei and ZTE (Burwell and Propp 2020, p. 7; see also Monsees and Lambach, this issue, on 5G and EU digital sovereignty). This, of course, has cybersecurity implications for the EU given the different levels of exposure to risk (penetration) from foreign vendors. Such issues of national divergence (and culture) within the EU also apply to other critical policy areas of digital sovereignty, including digital taxation and defence (Csernatoni 2021, p. 2). What these examples demonstrate then, is that vertical delineation of the concept can come up against national practice (and interests) even when common EU

guidelines, monitoring tools and competences exist, impacting on the credibility (and realisation) of the EU's ambition of technological sovereignty.

Some authors have called for "rethinking the governance mechanisms" related to creating an EU digitally sovereign environment to strengthen "the interaction between independent regulatory networks in order to promote collaboration and joint-decision making on digital topics" (Madiega 2020, p. 8; see also Wagner and Ferro 2020). This is not to say that challenges do not exist to constructing, protecting and projecting the EU's digital sovereignty but that there are clearly also opportunities through exploiting its current technological, regulatory and political competences and creating new powers and enhanced capacity and capability, to act in a "smarter" way in the geopolitics of digitalisation (Shapiro 2020, pp. 11–13, Fiott 2021, p. 14).

(b) What partnerships, principles, processes, and/or norms must be established to ensure the autonomy of the sovereign?

The EU is involved in numerous multilateral and bilateral processes that shape the cyber domain. Prominent among these have been the bilateral cyber dialogues with like-minded strategic partners such as the US and Japan as well as with those that are considered a systemic rival, such as China (Renard 2018). The EU also participates at various levels of governance where cyberspace is discussed. At the global level, for example, through the United Nations Group of Governmental Expert (UNGGE) and Open Ended Working Group (OEWG) processes that deliberate and have agreed on global norms of state behaviour and through enhancing cooperation with NATO; and at a regional level, through engaging with the ASEAN Regional forum, the African Union and the Organisation of American States through initiatives that seek to advance capacity building, construct norms and promote and diffuse Confidence Building measures (CBMs). To this end, the important question becomes that of how the EU's claims to sovereignty translate to the need for continued and enhanced cooperation in the cyber domain in order to ensure EU principles, interests, norms and values are upheld and diffused.

The rapid ascent of technological sovereignty as a leading concept in the EU's toolbox coincided with Brussels' greater affirmation of geopolitics as a key factor in its decision-making rationale. The backdrop of an intensively competitive and potentially dangerous world contributes to legitimising the EU's move towards being sovereign, while also shaping its external engagement. In this sense, they are mutually reinforcing: a sovereign EU and a geopolitical world. Within this order, as boldly remarked by the European Commissioner Thierry Breton, "Europe acts like a strategist rather than just a market. It remains open, but on its own terms. It makes its own choices and draws up its own rules, and is not afraid of imposing them on its partners" (Breton 2021). Acting strategically in the technological domain involves, first and foremost, setting standards: "We must become standard-makers, and not just standard-takers" (Breton 2021). At the same time, the EU should not be afraid of imposing its standards on its partners, it also has "a responsibility towards the international community: a duty of solidarity, of sharing, of fairness" (Breton 2021). The potential incompatibility between imposing EU's standards in the technological domain and "also playing for 'Team World'" (Breton 2021) is diluted in a mountain ridge metaphor,

> where our values and our interests meet; where the "soft power" that characterises us meets a new "hard power". A "hard power" that we also want to infuse the European Union with to establish ourselves as a partner – but one that is proud of its strengths and ready to defend them in a fiercely competitive global scene. (Breton 2021)

These remarks came weeks after the EU foreign ministers discussed the geopolitics of new technologies in the Foreign Affairs Council. In the summary of this meeting, it was asserted that these technologies are "a driver of geopolitical competition and global influence, being used by foreign actors to manipulate the information environment, influence the public debate, and interfere in democratic processes" (Council of the European Union, 2021b). As a response, the importance of the EU acting as a "regulatory power" was once again emphasised, not just for domestic purposes, but also so that it can "influence global norms and standards" while also ensuring "that the system remains open, human-centred and based on the rule of law" (Council of the European Union, 2021b). The potential paradox between imposing one's will and ensuring the system remains open is not acknowledged as a potential problem. Rather, working with like-minded partners is offered as solution that will help to consolidate such an agenda, as visible in the deeper partnerships and agreements with Japan and South Korea in relation to the adoption of the EU's GDPR rules and norms (Christou and Ji Soo 2021, Christou and Raska, 2021).

As part of this discussion, the Council approved Conclusions on "A Globally Connected Europe", where it brings together multiple policies – from the European Green Deal to an EU Space Programme – as part of a connectivity agenda. Although not directly referred to as part of the EU's approach to technological sovereignty, the Council starts by considering "that ensuring a geostrategic approach to connectivity has long-term implications for advancing the EU's economic, foreign and development policy and security interests and promoting EU values globally" (Council of the European Union, 2021a), before listing a number of actions for the Commission to undertake. It is once again clear that if sovereignty is the ordering concept for the EU's actions, geopolitics (or geostrategy in this case) is the external context that justifies it.

Internationally, the EU remains a strong advocate of a "global, open and interoperable Internet" (EEAS, 2019). That much was communicated in its first statement at the first session of the UN General Assembly OEWG on Developments in the Field of ICTs in the Context of International Security. But there is little in the promotion of those principles the EU can ensure through regulation. On the contrary, and as argued by Komaitis (2021), if anything regulation can have a fragmenting effect, as visible with GDPR, which has created "an extra-territorial effect" by being applicable anywhere in the world as long as it involves European citizens. In that sense, there is an internet for Europeans, and one for everyone else. This is what Kieron O'Hara and Wendy Hall (2021) have called the "Brussels Bourgeois Internet", one of the four internets they've identified as being in place at the moment.[6] Also, if anything, the articulation to sovereignty, even if the concept is used differently, helps to reinforce the legitimacy of those – particularly authoritarian regimes – that use it to justify the domestic control, repression, suppression and conditioning of their own citizens, while geo-restricting access to multiple services and websites in the name of national security (Mueller 2020).

Related and also important for the EU is to avoid exacerbating geopolitical tensions in the quest for sovereignty. As explained by a European diplomat, "a key issue is whether

the EU and its Member States are ready to defend that technological sovereignty in relation to other states". To this end, the EU's construction of its digital sovereignty has been driven by an increasing unease related to US digital dominance (and abuses therein) and heightened threat perceptions when it comes to Chinese digital investments and products, but there exists a tension between achieving European digital sovereignty and ensuring that at a more granular level, incentives to cooperate – where required – are maintained.

Conclusion

The EU has embraced and endorsed the concept of sovereignty in the technological domain, even if it has failed to clearly distinguish between technological and digital sovereignty.[7] In embracing the concept, it has taken performative steps with potential far-reaching consequences. Internally, it has re-centred the multiple policies and initiatives related to cyberspace, cybersecurity and the digital realm around the idea of sovereignty. Concepts such as resilience and strategic autonomy are directly associated, and one might argue underpin and are vehicles for the EU's sovereign ambitions. It has also (re)prioritised such ambitions in terms of what policy areas will more directly contribute to help the EU to achieve its strategic sovereign ambitions. Furthermore, it firmly marks the ground regarding Member States in terms of what sovereignty means in Europe. It is a concept that is necessarily multi-level and operates across a number of spaces and mandates, but at the same time has aggregating ambitions, thus impacting on questions of both authority and legitimacy in constructing and indeed implementing and projecting sovereignty in the digital realm.

Externally, the sort of technological sovereign the EU is constructing has implications for its ability to act and influence through diplomacy and in terms of security and its ambitions relating to a resilient and safe digital market. Indeed, how the EU constitutes itself as a technologically sovereign actor will also impact the means through which it seeks to achieve it, that is, strategic autonomy. And this is happening, in the context of an increasingly competitive geopolitical environment, where differing constructions and conceptions of digital, data and technological sovereignty conflict with the values and strategic and economic interests that the EU is striving to project and protect in the digital sphere.

To this end, the EU's construction of itself as technologically sovereign is taking place in relation to its internal competences and rules and externally in relation to those it constructs as the Others that challenge its norms, interests and values. The increasing rivalry between the US and China and the COVID-19 pandemic have further accelerated the need for the EU to ensure that it remains secure, safe and resilient, and more importantly, that it is able to do this through reducing technological and economic dependencies. Being technologically sovereign then, is reliant on partnership bilaterally and at the multilateral level to agree solutions to the global problem of security in cyberspace.

As Milton Mueller highlights, "We can have a globally compatible internet, or we can strive to align digital technology with political borders. We cannot do both" (Mueller 2020, p. 798). In that regard, willingly or unwillingly, the EU's delineation of sovereignty is an exclusionary exercise, not only in that its views are different from those of other key actors in cyberspace – notably Russia and China – but in that, they are fundamentally

incompatible. The challenge for the EU if we accept the premise and language of technological sovereignty in the post-traditionalist sense, is to be able to diplomatically navigate the tensions that this might bring with it in a geostrategic environment where cyberspace has become a key area for competition and confrontation, as well as cooperation. This is not an impossible task but will involve the EU thinking more carefully about how it can ensure security and resilience in its approach to cybersecurity, while also acknowledging that its sovereignty moves will have differentiated effects on the very players – democratic and authoritarian – that it will remain reliant upon to achieve its own open strategic autonomy when it comes to cyberspace and other related policy dimensions.

Notes

1. For a broader discussion and typology, see Bellanova *et al.*, this issue, as well as Krasner 1999.
2. In this paper, we take the EU to be a unitary actor, capable of speaking and acting holistically. Although we recognise there may be different views within its bodies, member states, and multiple committees and agencies, those would only be relevant for this article if they were part of the official discourse, which they are not.
3. Indeed, in her State of the Union address von der Leyen stressed the need to

> … make this Europe's Digital Decade. We need a common plan for digital Europe with clearly defined goals for 2030, such as for connectivity, skills and digital public services. And we need to follow clear principles: the right to privacy and connectivity, freedom of speech, free flow of data and cybersecurity. (European Commission 2020)

4. For EU digital goals also see European Commission, 2021.
5. Taken from – https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
6. The others being the Silicon Valley Open Internet, the DC Commercial Internet and the Beijing Paternal Internet (O'Hara and Hall 2021).
7. In the words of a diplomat interviewed for this paper, "maybe the first thing we need to do is to see if we all agree on the same definition of technological sovereignty" (European Diplomat, 2021).

Disclosure statement

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

Funding

This work was partially supported The Leverhulme Trust [grant number RF-2019-466].

Notes on contributors

Andre Barrinha is a Senior Lecturer in International Relations at the University of Bath and a Leverhulme Trust Research Fellow (2019–2021). His work is published in journals such as *International Affairs, Mediterranean Politics, Third World Quarterly, Journal of Common Market Studies and Journal of European Integration*. He is also one the authors of *International Relations Now and Then* (Routledge, 2nd ed.). Dr Barrinha is currently working on cyber-diplomacy as an emerging practice in international relations. In 2019, he was awarded the Best Article in Global Affairs Award for a co-authored piece with Thomas Renard on cyber diplomacy and the English School. He has recently been appointed a member of the UK Multi-Stakeholder Advisory Group on Cybersecurity. Between 2016 and 2018, he was one of the founders and conveners of the British International Studies Association European Security Working Group.

George Christou is Professor of European Politics and Security at the University of Warwick, UK. He has published widely on European Politics and Security and he is the Editor for Palgrave's New Security Challenges Series. His most recent books include *Global Networks and European Actors: Navigating and Managing Complexity,* (Routledge, 2021 edited with Jacob Hasselbalch); *Global Standard Setting in Internet Governance* (Oxford University Press, 2020 with Alison Harcourt and Seamus Simpson); *The European Union and Cybersecurity: Adaptation and Resilience in Governance Policy* (Palgrave Macmillan, 2016). His latest articles include: 'Interest group lobbying in the European Union: privacy, data protection and the right to be forgotten' (2021, Comparative European politics with Imir Rashid); 'The Collective Securitisation of Cyberspace in the European Union' (2018, West European Politics); 'The Challenges of Cybercrime in the European Union' (2018, Journal European Politics and Society). He is currently engaged in CYDIPLO – European Cyber Diplomacy, a Jean Monnet Network co-funded by the Erasmus+ Programme of the European Union (September 2020–Aug 2023).

References

Adonis, A., 2020. *European digital sovereignty: EU's projection of normative power?* Global Media and Technologies Culture Lab, Network Sovereignty Blog, 9 September. Available from: https://globalmedia.mit.edu/2020/09/09/european-digital-sovereignty-eus-projection-of-normative-power/ [Accessed 22 June 2022].

Barlow, J.P., 1996. *A declaration of the independence of cyberspace*. Electronic Frontier Foundation, 8 February. Available from: https://www.eff.org/fr/cyberspace-independence [Accessed 14 November 2017].

Barrinha, A., and Renard, T., 2020. Power and diplomacy in the post-liberal cyberspace. *International affairs*, 96 (3), 749–766.

Bartelson, J., 2008. Sovereignty before and after the linguistic turn. In: Rebecca Adler-Nissen, and Thomas Gammeltoft-Hansen, eds. *Sovereignty games. Intrumentalizing state sovereignty in Europe and beyond*. London: Palgrave, 33–46.

Bauer, M., and Erixon, F., 2020. *Europe's quest for technology sovereignty: opportunities and pitfalls.* European Centre for International Political Economy, ECIPE Occasional Paper, 02/2020, 1–42.

Bellanger, P., 2012. De la souveraineté numérique. *Le Débat*, 170 (3), 149–159.

Borell, J., 2020. *Why European strategic autonomy matters.* From the blog, European External Action Service, 3 December. Available from: https://eeas.europa.eu/headquarters/headquarters-homepage/89865/why-european-strategic-autonomy-matters_en [Accessed 14 September 2021].

Breton, T., 2021. *The Geopolitics of Technology*, 27 July. Available from: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/geopolitics-technology_en [Accessed 14 September 2021].

Burwell, F.G., and Propp, K., 2020. 'The European Union and the search for digital sovereignty: building "fortress Europe" or preparing for a new World?' Issue Brief, Atlantic Council, Future Europe Initiative.

Carr, M., 2015. Power plays in global internet governance. *Millennium: journal of international studies*, 43 (2), 640–659. doi:10.1177/0305829814562655.

Carrapico, H., and Barrinha, A., 2017. The EU as coherent (cyber) security actor? *JCMS: journal of common market studies*, 55 (6), 1254–1272.

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, e-book. Available from https://ai-regulation.com [Accessed December 2020].

Christou, G., and Raska, M., 2021. EU–ASIA cybersecurity cooperation: paths and patterns. In: Thomas Christiansen, Emil Kirchner, and Tan See Seng, eds. *The European union's security relations with Asian partners* (pp. 209–230). Cham: Palgrave Macmillan.

Christou, G., and Soo Lee, J., 2021. EU–ROK cooperation on cyber-security and data protection. In: Nicola Casarini, ed. *EU-Korea Security relations* (pp. 55–77). London: Routledge.

Council of the European Union, 2021a. *A globally connected Europe*. Council Conclusions, Brussels, 12 July, 10629/21.

Council of the European Union, 2021b. *Foreign affairs council*, 12 July. Main results. Available from: https://www.consilium.europa.eu/en/meetings/fac/2021/07/12 [Accessed 14 August 2021].

Couture, S., and Toupin, S., 2019. What does the notion of "sovereignty" mean when referring to the digital? *New media & society*, 21 (10), 2305–2322.

Csernatoni, R., 2021. The EU's rise as a defense technological power: from strategic autonomy to technological sovereignty. *Carnegie Europe*, 12 August 2021. Available from: https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty/$ [Accessed 12 August 2021].

European Commission, 2019. Speech by President-elect von der Leyen in the European parliament plenary on the occasion of the presentation of her college of commissioners and their programme, 27 November. Available from: https://ec.europa.eu/commission/presscorner/detail/es/speech_19_6408 [Accessed 15 September 2021].

European Commission, 2020a. State of the Union address by President von der Leyen at the European parliament plenary, 16 September. Available from: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655 [Accessed 15 September 2021].

European Commission, 2020b. Communication from the commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'EU Security Union Strategy', Brussels, 24.7.2020, COM (2020) 605 final.

European Commission, 2020c. Communication from the commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European Strategy for Data', Brussels, 19 February, 2020, COM (2020) 66 final,.

European Commission, 2021. *2030 Digital Compass: the European way for the Digital Decade*, 9 March 2021. Available from: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en [Accessed 15 September 2021].

European Commission and High Representative of the European Union for Foreign Affairs and Security Policy/Vice-President of the Commission, 2013. Cybersecurity strategy of the EU: an open, safe and secure cyberspace, Brussels, 7 February.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2017. Joint communication to the European parliament and the council resilience, deterrence and defence: building strong cybersecurity for the EU, JOIN/2017/0450 final.

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, 2020. Joint communication to the European Parliament and the Council, "The EU's Cybersecurity Strategy for the Digital Decade", Brussels, 16.12.2020 JOIN (2020) 16 final, 19.

European Council, 2019. European Council conclusions, Brussels, 21–22 March 2019. Available from: https://www.consilium.europa.eu/en/meetings/european-council/2019/03/21-22/ [Accessed 14 September 2021].

European Council, 2020a. European Council conclusions, Brussels, 1–2 October 2020, EUCO 13/20, CO EUR 10, CONCL 6.

European Council 2020b. European Council conclusions, Brussels, 10-11 December 2020, EUCO 22/20, CO EUR 17, CONCL 8.

European Council, 2021. Statement of the members of the European Council, Brussels, 25 March 2021, SN18/21.

European Council and Council of the EU, 2021a. Video conference of the members of the European Council, 25–25 March 2021.

European Council and Council of the EU, 2021b. *A digital future for Europe: EU leaders stress need to enhance the EU's digital sovereignty*. Available from: https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/ [Accessed 14 September 2021].

European Council and Council of the European Union, 2019. A new strategic agenda for the EU: 2019-2024. Available from: https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/.

European Diplomat, 2021. *Interview with A. Barrinha*. MS Teams. 16 July.

European External Action Service, 2017. *Shared vision, common action: a stronger Europe: a global strategy for the European Union's foreign and security policy*. Publications Office.

European External Action Service, 2019. EU general statement. OEWG on cyber, First Session, New York, 9 September. Available from: https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/EU(General(Statement(to(the(OEWG(on(Cyber%2C(First(Session.pdf [Accessed 14 September 2021].

European Parliament, 2019. *Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them*. European Parliament, 2019/2575(RSP), 12 March 2019. Available from: https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1577382&t=d&l=en [Accessed 14 September 2021].

European Political Strategy Centre, 2019. Rethinking strategic autonomy in the digital age. EPSC Strategic Notes, Issue 30, July 2019.

Fiott, D., 2021. *European sovereignty: strategy and interdependence*. Paris: European Union Institute for Security Studies. Chaillot Paper/169, July 2021.

Gammeltoft-Hansen, T., and Adler-Nissen, R., 2008. An introduction to sovereignty games. In: R. Adler-Nissen, and T Gammeltoft-Hansen, eds. *Sovereignty games. Intrumentalizing state sovereignty in Europe and beyond*. London: Palgrave, 1–17.

Hobbs, C., 2020. Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry, *Essay Collection, European Council on Foreign Relations*, 30 July. Available from: https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/ [Accessed 8 September 2021].

Ilves, L., and Osula, A.-M., 2020. The technological sovereignty dilemma–And How New technology Can offer a Way Out. *European cybersecurity journal*, 6 (1), 24–35.

Kello, L., 2018. *The virtual weapon and international order*. New Haven: Yale University Press.

Komaitis, K., 2021. Europe's ambition for digital sovereignty must not undermine the internet's values. *Computer fraud & security*, 2021 (1), 11–13.

Krasner, S.D., 1999. *Sovereignty and its discontents, in power, the state, and sovereignty: essays on international relations*. London: Routledge, 179–180.

Madiega, T., 2020. Digital sovereignty for Europe, briefing, European Parliamentary Research Service, Ideas Paper, PE651.992, July 2020.

March, C., and Schieferdecker, I. 2021. Technological sovereignty as ability, not autarky, CESifo Working Paper No. 9139. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3872378.

Mills, R.E., 2014. The pirate and the sovereign: negative identification and the constitutive rhetoric of the nation-state. *Rhetoric and public affairs*, 17 (1), 105–136.

Moerel, L., and Timmers, P. 2021. Reflections on digital sovereignty, *research in focus*, EU Cyber Direct. https://eucyberdirect.eu/research/reflections-on-digital-sovereignty [Accessed 22 June 2022].

Mueller, M.L., 2020. Against sovereignty in cyberspace. *International studies review*, 22 (4), 779–801.

O'Hara, K., and Hall, W., 2021. *Four internets. data, geopolitics, and the governance of cyberspace*. Oxford: OUP.

Pohle, J., and Thiel, T., 2020. Digital sovereignty. *Internet policy review*, 9 (4), 1–19.

Renard, T., 2018. EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European politics and society*, 19 (3), 321–337.

Shapiro, J., 2020. Introduction: Europe's digital sovereignty. In: C Hobbs, ed. *Europe's digital sovereignty: from rulemaker to superpower in the age of US-China rivalry* (pp. 6–29). Essay Collection, European Council on Foreign Relations. 30 July. Available form: https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/ [Accessed 8 September 2021].

Thumfart, J., 2021, The COVID-crisis as catalyst for the norm development of digital sovereignty. Building barriers or improving digital policies?. https://doi.org/10.2139/ssrn.3793530

Timmers, P., 2019. Strategic autonomy and cybersecurity, policy in focus, *EU Cyber Direct*, 10 May 2019. Available from: https://eucyberdirect.eu/research/strategic-autonomy-and-cybersecurity [Accessed 14 September 2021].

Wæver, O., 2009. Discursive approaches. In: Antje Wiener, and Thomas Diez, eds. *European integration theory* (2nd ed.). Oxford: Oxford University Press, 163–180.

Wagner, B., and Ferro, Carolina, 2020. *Governance of digitalization in Europe*. Gütersloh, Germany: Bertelsmann Stiftung.

Walker, N., 2008. The variety of sovereignty. In: Rebecca Adler-Nissen, and Thomas Gammeltoft-Hansen, eds. *Sovereignty games. Intrumentalizing state sovereignty in Europe and beyond*. London: Palgrave, 21–32.

Werner, W.G., and De Wilde, J.H., 2001. The endurance of sovereignty. *European journal of international relations*, 7 (3), 283–313.

Wolff, G., Poiters, N., and Weil, P., 2021. Sovereignty and digital interdependence. In: D. Fiott, ed. *European sovereignty: strategy and interdependence* (pp. 16–22). Paris: European Union Institute for Security Studies. Chaillot Paper/169, July.

Wu, T., 1997. Cyberspace sovereignty? – The internet and the international system. *Harvard Journal of Law & Technology*, 10 (1997), 647. Available from: https://scholarship.law.columbia.edu/faculty_scholarship/2227.

Youngs, R., 2021. The EU's strategic autonomy trap. *Carnegie Europe*, 8 March 2021. Available from: https://carnegieeurope.eu/publications/83955 [Accessed 8 March 2021].