*Dear reader,*

*I am very grateful to you for taking the time to read this rough paper. It is work in progress. Some background: this paper is one of four working papers that we in the research project “Solixg: the social life of XG, digital infrastructures and the re-configuration of sovereignty and imagined communities”, have committed to deliver this year. It is not a paper that will be published but aims to provide the project team with a common ground to build and develop further research. As it is now, I am just reading through a lot of literature on digital sovereignty and the text you receive is a map of how I, at this moment, perceive the landscape. I would love to have your feedback on the ideas that are in progress in the text. I wish I had more developed thoughts in the last section, but this is where I am now. Perhaps, we can develop more thoughts on the topic during the seminar. Also, I would love your input on how I could develop a migration angle on the topic of digital sovereignty for further empirical research.*

*Thank you,*

*Mauricio*

**Working paper: literature review on digital sovereignty**

**Introduction**

In 2020, the European commission presented a recovery and resilient stimulus package that aimed to rebuild and strengthen Europe economically after the recession due to the covid-19 pandemic. As a solution to lockdowns taken place in most countries, the digital activity drastically increased; recovery and resilience towards future crises, it seems, is not without strengthening the digital capacity and more independent of digital infrastructures. According to the President of the European commission Ursula von der Leyen, this package, called “NextGenerationEU”, is, thus, “about Europe’s digital sovereignty, on a small and a large scale” (von der Leyen 2020). Digital technologies and more recently, Europe’s digital sovereignty have become main themes in EU policies the last few years. Between 2019 and 2022, the president of the European commission, the president of the European council and the High representative of the union of foreign affairs and security policy, all referred to digital sovereignty in their public speeches (Bellanova, Carrapico and Duez, 2022, p. 337). Traditionally reserved for nation states, the use of the term sovereignty within the digital sphere appears as somewhat peculiar. The slightly antithetical use of the term has drawn scholarly attention recently, driving researchers to pose questions about what sovereignty means in the realm of the digital, and how and why the digital is conceived as a key strategic domain for governance. To come to grips with what digital sovereignty refers to and to better grasp what the literature makes out of it, this paper reviews the academic literature on digital sovereignty. It does so, first, by summarizing how the academic literature conceptualizes digital sovereignty in relation to other closely related terms such as data sovereignty, and cyber sovereignty. Second, it reviews the literature analyzing the increased usage of the term digital sovereignty within a European context and how it has reached the center of EU policy. Third, the paper offers a critical conceptualization of digital sovereignty. By putting digital sovereignty side by side with critical understandings of the classical concept of sovereignty, while also relating it to imaginaries of community and nationhood (Anderson, 2016), ethnos and demos (Balibar, 2004), the paper purposes to present a critical analytical path to further study digital sovereignty.

Even though, this paper will refer to critical understandings of the traditional concept sovereignty, it will not deal with this concept in detail. Yet, we need to have some kind of understanding of what sovereignty means traditionally. In simple terms, sovereignty refers often to the exclusive power of an authority within a given territory, represented by the state (Jablonski and Powers, 2015, p. 155). A bit more elaborated, still very sketchy, following Wendy Brown (2010), who in turn draws on classical thinkers of sovereignty such as Thomas Hobbes and Jean Bodin, and later, Carl Schmitt, sovereignty consists of six features. 1) Supremacy: there is no higher authority than the ruling body. 2) Perpetuity: there is no term limit for authority. 3) Decisionism, the ruling body is not bound to law. 4) Absoluteness and completeness. Sovereign power cannot be probable or partial 5) Nontransferability: the sovereign power cannot be conferred without canceling itself. And 6) the sovereign power is delineated to a specified jurisdiction, a territory (Brown, 2010, p. 22).

Brown’s description of sovereignty should be understood as ideal typical. In contrast to this definition, sovereign borders, territory, and supreme power, are always challenged and contested by people on the move, flows of ideas and goods. Accordingly, Brown asserts that the walls built towards of the end of the 1900s and the beginning of the 2000s, did not target armed forces of other sovereign states but non-state transnational actors such as individuals, organizations, groups, movements, and industries, suggesting that the new walls are signs of a post-Westphalian order (2010, p. 21). However, with the escalation of the Russian invasion of Ukraine in 2022 and the growing tension between China and the United States, we might need to revisit Brown’s assertation about waning sovereignty.

Similarly, the literature on digital sovereignty departs from the image of a disintegrated and eroded state. In this understanding, global computation (Bratton, 2015), constantly challenges the nation-state’s territorial boundaries and, to a certain extent, escapes governance and re-configures geopolitical landscapes. Interestingly, analogues with the development in political international relations, tracing the evolution of digital sovereignty from its birth to the present day, showcases a progression towards the return to a Westphalian order (Mueller, 2020).

**Methodology**

**The digital sovereignty, data sovereignty and cyber sovereignty**

The concept of digital sovereignty has emerged as a respond to various intertwined developments and discourses around global computation and waning sovereignty, given way for a plethora of different understandings and discourses of the term (Couture and Toupin, 2019, p. 2306; Hummel et al., 2021, p. 1; Pohle and Thiel, 2021a, p. 50). To unpack some of the ascribed understandings and usages of digital sovereignty, I will juxtapose the term with data sovereignty and cyber sovereignty.

Following Pohl and Thiel, digital sovereignty emerged first as a discursive concept to respond to the growing techno-political challenges and threats to state sovereignty stemming from ideas and policy ideals framed as cyber exceptionalism and multi-stakeholder Internet governance (Pohle and Thiel, 2021, p. 50). The concept of cyber exceptionalism became particularly popular during the advent of the commercial Internet in the 1990s and has ideological roots in cyber libertarianism (Pohle and Thiel, 2021, p. 51). According to this a cyberlibertarian vision, digitally mediated forms of politics would decentralize political organization and create a new and autonomous political space, less bounded by territories and sovereign states, independent of governmental interferences (ibid). Multi-stakeholder Internet governance poses a related but less confrontative threat to state sovereignty. The vision of multi-stakeholderism stems from the early 2000s and onwards and relies on principles and policy-frameworks proposing openness and inclusion on an international level, bottom-up collaboration and consensual decision-making to counteract centralized policy (Hofmann, 2016; Pohle and Thiel, 2021). Although, ideas and ideals of decentralization within the digital realm continue to thrive, perhaps most pertinent and aggressively formulated within the crypto-currency space (see e.g. Pistor, 2020), it is mostly the concentration of power to corporate actors within commercial internet, state-surveillance, and cyber security, that has spurred the major evolution of the concept digital sovereignty.

Digital sovereignty has gained traction as it opposes the corporate powerhouses, commercialization of internet, creating platforms harvesting personal data for profit and who have come to own vital material and immaterial structures, threatening democratic sovereignty (see e.g. Zuboff, 2019; Pohle and Thiel, 2021). With respect to the global IT conglomerates such as Alphabet, Meta, or Alibaba, “data sovereignty” is a related term (if not synonymous). According to a comprehensive quantitative review of the concept, the candidate meaning refers to control, ownership, and claims to data, by individual consumers, or societies or states (Hummel *et al.*, 2021, p. 15). Even if there is some slippage between digital sovereignty and data sovereignty, there is a preponderance to use data sovereignty as referring to primarily the control of data, and only data. A search on “data sovereignty” in the database *Scopus*, bolsters this assumption. We see that the use of the concept relates to topics such as health data (Pericàs-Gornals et al., 2022), data archives (Adelson and Mickelson, 2022), data sharing (Jacoby *et al.*, 2021) and the right to one’s data (Calzada, 2021). These articles points towards the use of data sovereignty as predominantly emphasizing “data” as processed and stored/shared information.

Furthermore, the literature on data colonialism, intimately connected to the literature on data sovereignty, uses the same conceptualization of data. Following Mouton and Burns (2021, p. 1891), Roberts and Montoya write that data colonialism “concerns the abstraction of life into bits and bytes, whereas digital colonialism encompasses data but also the infrastructure and hardware that make up the digital world and the connection to the internet (2022, p. 2)”. Hence, a rough reading of the literature, allow us to separate data sovereignty as mainly targeting data from digital sovereignty, which also includes technologies and infrastructures. Interestingly, as Couture and Toupin (2019, p. 2313) observe, the use of data sovereignty, or digital sovereignty, outside the US and in particular, the global south, has positive connotations while the use of the terms in the US, has negative connotations. From the perspective of power asymmetries and a potential explanation to the different connotation, the term data colonialism could not be more telling. Sovereignty outside the US means evading data imperialism or colonialism. Within the US, the negative connotations reflect a tension between decentralization and centralization. Another tension that exists within nations is how populations are represented and for what purposes the state collects data. The term indigenous data sovereignty highlights this tension, referring to sovereignty as autonomy and emancipation (Taylor and Kukutai, 2016; Roberts and Montoya, 2022).

Even if there are overlaps between digital sovereignty and cyber sovereignty, the latter is in this literature review invoked to illustrate the third dimension connecting the digital with sovereignty. While data sovereignty, as described above, refers to individuals’ right or populations’ right to their data and privacy, cyber sovereignty refers to a nation’s, or a region’s, ability to take autonomous action and take decisions concerning its digital infrastructures and deployment of technology (Pohle and Thiel, 2021, p. 55). In this sense, cyber sovereignty is strongly linked to territoriality, which is at the core of the more traditional definition of sovereignty. A critical moment was the Snowden revelations in 2013. Snowden leaked documents disclosing the National Security Agency’s global surveillance practices (Barrinha and Christou, 2022, p. 359). Against the background of the unveiled US’ claims to global hegemony in the cybersphere with borderless global surveillance initiatives, cyber sovereignty speaks to issues of state’s protection against external threats. However, cyber sovereignty is not all about cyber security and territorial defensive concerns but as Yu Hong and Thomas Goodnight describe with the example of China’s shifting justification of cyber sovereign policies, it implies also globalist development ethos (2020, pp. 16–17). Continuing with the case of China, the failed attempt to reach an agreement with American companies on respecting every country’s internet sovereignty in 2014, has led the Chinese state to move towards finding a middle-ground between border-enforcement and opportunity-looking imperatives regarding their internet governance (Hong and Goodnight, 2020, p. 18). After the first failure to reach an agreement at the Wuzhen Summit, during the second edition of the conference, Xi Jinping, established a multilateral governing structure, presenting a vision of transnational structures of communication relations, opportunities, resources, and protocols. This vision portraits China as a big internet nation, realized thanks to various stakeholders and the integration of ideas and technological initiatives from around the world. Hence, as the Westphalian order of sovereign state, already been eroded due to the participation in the cybersphere, China’s new approach turned cyber sovereignty from a notion of a territory-based devise into a global development vision (Hong and Goodnight, 2020, pp. 18–19). Much of the literature on cyber sovereignty deals with geopolitics and involves the political and economic relations between China, the US and Russia.

**European digital sovereignty**

As seen in the section above, since the advent of popular internet, technological powerhouses, and surveillance schemes, the term sovereignty has made a comeback in the political field. A combination of waning sovereignty of nation-states (Brown 2010), the simultaneous emergence of a new digital territory and the declaration of the non-state sovereign and autonomous space (Barlow), has put forward calls for re-configurations of state’s role within the digital realm through internet governance. The use of digital sovereignty within EU appears at first a bit peculiar. In a more traditional understanding, the term sovereignty rhymes bad with EU’s principle of national procedural autonomy. Still, during the last decade, sovereignty within the realm of the digital saturates EU policies (see e.g. Bellanova, Carrapico and Duez, 2022). In this section I will describe how the literature on digital sovereignty portraits EU’s argumentation and turn towards a digital sovereignty that some define as a middle-ground between the US’ more anarchic approach to digital regulations and China’s more “heavy-handed” state control advocacy (e.g., Hobbs 2020). This literature helps us to further understand the conceptualization of digital sovereignty in relation to data sovereignty and cyber sovereignty.

The increased use of digital sovereignty in EU policy represents, in part, a desire to compensate for the insufficient development of software and hardware during the past decades, and the dependency on the US and China, according to Martin Kaloudis (2022, p. 275). The discourse revolves around obtaining control of EU digital infrastructure and technological production to strengthen EU’s economic competitiveness but also to enforce EU citizens cybersecurity, which goes lost on the dependency on “foreign” service providers (Farrand and Carrapico, 2022, p. 435). Despite the frequent use of it in policy, there is no common definition of digital sovereignty (Kaloudis, 2022, p. 276). Perhaps precisely due to its vagueness, the use of the term expresses an interesting tension between a definition more akin to cyber sovereignty, and an individual-oriented approach towards data security and privacy. This might be, following Georg Glazse et al., a result of the many European voices trying to merge the geopolitical demands of territorial closure in the global economic competition and desire to build protective cyber walls and autonomous digital infrastructure, underpinned by the notion of “European values” (2023, p. 923). With a combination of regulatory power, underpinned by value-oriented legitimization, the EU is currently trying to engineer a third option in the battle for profit in the current digital transformations (Glasze *et al.*, 2023, p. 932). In short, the two main themes that reoccur in the literature is economic competition and technological rivalry, on the one hand, and cyber security and privacy, on the other.

The discourse around technological rivalry and economic competition is not new. Linda Monsees and Daniel Lambach argues, drawing on paper by Andrew Barry and William Walters (2003), that technological infrastructures have been instrumental for European integration ever since the start of the European Community and that technological capabilities been central, at least since the establishing of EUROTOM (European Atomic Energy Community) (2022, p. 380). With the advent of internet and digital infrastructure, the discourse has taken on yet another layer and presents a different rival. Whereas during the Cold war, Europe was caught in the fire between USA and Soviet Union, it is now caught between USA and China. This position between two competitive superpowers highlights Europe’s small market shares in the cyber sphere and digital infrastructures. For instance, today, it is only a small number of companies worldwide that can provide 5G equipment, produce high-end semiconductors and offer cloud computation capacity (Monsees and Lambach, 2022, p. 379). These are mostly American companies such as Google, Apple, Amazon and Intel, or, Chinese, such as Alibaba, Tencent and Huawei. As these companies, through their services which customers have integrated into their everyday lives, become not only an economic threat to the European internal market but also a democratic as they own a direct unmediated link to their customers. Digital sovereignty has since several years now been discussed but only intensified the last few years. Pierre Bellanger, CEO of the French radio station SkyRock, has since 2011 in various articles and interviews, popularized the discussion about the loss of national sovereignty because of state’s, namely the US, and large companies appropriating data. More dramatically formulated, Bellanger argued that France had become a vassal of the cyber empire USA, and that Europe had chosen a path towards digital subordination, provincialization and colonization (Christakis 2020). This vocabulary spread to French politicians and in 2013, Catharine Morin-Desailly authored a report released by the European Affairs Committee of the French Senate called *L’Union européene, colonie du monde numérique?* The literature itself does not use this term but it is a term that circulates among politicians and companies to some degree (see Hobbs 2020). Within the discourse, the issue of “neocolonial” dependence on American big tech companies is not merely an economic problem. Social media has gain significant sway within the realm of politics, enabling foreign actors to spread disinformation and undermine democratic institutions (Shapiro in Hobbs 2020:8-9; Monsees and Lambach, 2022, p. 379).

With the idea of the threat of erosion of democratic institutions, the discourse on digital sovereignty has increasingly become a matter of security. Here, Monsees and Lambach (2022) sees a shift in how digital sovereignty has been framed as an economic question to become increasingly an issue of security (2022, p. 388). The authors draw this conclusion by studying how EU position itself between USA and China through three cases representing different layers of digital infrastructures. The first case is Gaia-X, a Franco-germen initiative to secure and federate a cloud computing infrastructure that puts European values such as privacy at the forefront (Baur, 2023, p. 1). The project intends to create a platform where European companies can connect to data and cloud services adhering to European regulations (Baur, 2023, p. 15). Although, this is a private sector initiative, that in addition is having difficulties challenging global actors like Amazon or Alibaba, the EU sees it as an important step towards European digital sovereignty (Monsees and Lambach, 2022a, p. 383). The second case concerns the expansion of 5G infrastructures, which will most probably play a crucial role in the digital transformation of EU’s economy and society writ large. However, the use of the higher frequencies on the spectrum, which 5G technology uses, requires the installation of new kind of infrastructure, a technology that currently is dominated by five companies, Huawei, ZTE, Nokia, Ericsson, and Samsung. Many member states of the EU have formulated fears of integrating Chinese companies, such as Huawei and ZTE, as partners in the expansion of digital infrastructure due to fears of surveillance and espionage. Although, US companies are perceived here too as an economic threat to the expansion of European digital infrastructures, China is in addition perceived by the European Union member states as a security threat (Monsees and Lambach, 2022a, p. 385). The third case revolves around securing the production and the supply chains of semiconductors, which are small materials used in billions in chips to amplify electronic signals. These are essential in basically all electronic goods and digital devices. The semiconductor industry is truly globalized; it is said that one single semiconductor crosses 70 borders before reaching its end destination. Securing this industry is a precondition to become a competitive nation in the digital economy, an economy that grows with each year. Thus, EU, has identified this industry as essential in its path towards digital sovereignty (Monsees and Lambach, 2022a, p. 386). However, when it comes to semi-conductors, any form of independence is practically impossible due to this industry’s intricate and global specialized value chain. This is a recognized technological fact. Nevertheless, the European commission still drives claims about the need to become self-sufficient, in that process, depicting China as the core competitor and a threat, although China is neither self-sufficient or autonomous when it comes to the production of semiconductors (Monsees and Lambach, 2022a, p. 387).

At least two of these projects are part of the concrete (if not predominantly material) digital infrastructure. They not only identify infrastructural problem areas but also introduce ideas of potential solutions and paths towards digital sovereignty, even if the solutions are not realistic and rather creates a security imaginary (see e.g. Csernatoni, 2022). Together with these discussions, there are other policy amendments that influence the digital landscape in a less confrontative manner. For instance, the General Data Protection Regulation (GDPR) is an example of how EU can leverage access to the EU market and develop a framework encouraging the internal market while also promoting European values of integrity and privacy, which are portrait as European values (see Hobbs 2020:12). For Farrand and Carrapico (2022), policies regulating the internal market, and in continuation, the infliction upon external private actors to adapt to it, marks a shift from a governance characterized by “regulatory capitalism” to one characterized by “regulatory mercantilism”. While private actors always been part of the European commission’s regulatory effort, this shift tends to make a distinction between “domestic” and “foreign” actors, aiming to protect the European single market and closing-off cyberspace onto a European territoriality. Regulatory mercantilism refers to the commission’s desire to build a secure territory through accumulating data resources within the territory and using this power to set the norms and define values which hopefully will spread to the outside of EU territory (Farrand and Carrapico, 2022, p. 436).

I will end this section with two conclusions. The first is that the discussions around digital sovereignty seem to refer to an EU integration through the protection of digital infrastructures and the single market, which draws both on an economic and a security rationale. The second conclusion is that digital sovereignty refers to both material digital infrastructures as semiconductors, 5G-technology, and less material aspects of the digital sphere, such as policy regulations concerning the single market and data security.

**Continuities, overlaps, parallels**

The discussions about sovereignty in a quickly digitized world echo earlier ideas and social and economic geopolitical developments. Therefore, this last section will pay heed to continuities, overlaps and recurring patterns in discussions and developments in digital sovereignty, read through the lens of critical understandings of the more classical conceptualization of sovereignty. It centers around two main themes, which should be understood as potential analytical avenues. The first revolves around the process of deterritorialization and reterritorialization. The second focuses on how both sovereignty and digital sovereignty manufactures a territorial/cultural/social/political inside and an outside, and how the process of creating a robust inside is dependent on *an* outside and colonial infrastructures of extraction. Hopefully, this will prepare the ground to pose further questions about how re-configurations of sovereignty emerge and how digital technology impacts ways of imagining nationhood and community.

The first continuity (or, perhaps, *analytical parallel* is a better formulation) concerns one that could be framed as a continuous process of deterritorialization and reterritorialization both of thought and space, which lies at the heart of modern sovereignty. According to Michael Hardt and Antonio Negri, sovereignty is a European concept. It developed primarily in Europe in tandem with the evolution of modernity (Hardt and Negri, 2000, p. 70). In the origins of modernity, around the fifteenth century, no less than a revolution in though took place, in which a new immanent ontological knowledge liberated humanity from transcendental plane of thinking and the inherit relation between *man* and god (Hardt and Negri, 2000, p. 72). This revolution was unavoidably met by a counterrevolution that sought to destroy and dominate the new forces of emancipation and human dignity. Accordingly, modernity is defined by crises and violent conflicts between two modes of modernity, between the first movement of immanent, constructive, and creative forces, on the one hand, and the reactive counterrevolutionary transcendent power, on the other (Hardt and Negri, 2000, p. 76). Sovereignty emerged in this tension, in these conflicts. From the counterrevolution emerged a transcendent apparatus that sought to impose order on the liberated singularities, and what Hard and Negri calls “the revolutionary constitution of the multitude” (2000, p. 83). This new transcendent form of governing needed above all to guarantee its control over these revolutionary influences and movements to profit from its potential without imposing on them an old medieval transcendental model. The result was a transcendental political apparatus and a state-centered sovereignty (Hardt and Negri, 2000, p. 83). However, in the construction of state sovereignty lies a contradiction. As Hardt and Negri argues, there can only be one sovereign, the king, for instance (2000, p. 85). The sovereign is defined, as seen in the introduction, by its supreme power and cannot be questioned by the rule of others. This is an important assertion because states are still conceived as sovereign. The figure of a sovereign unified body consisting of a multitude of voices needs a foundation of values and beliefs. These values and sets of beliefs change over time and are closely related to, for instance, different forms of governing (sovereignty, discipline and governmentality) and technologies conditioning the dissemination of beliefs and ideas (e.g. print technology/print capitalism). Underneath these conditions lies the content of modern sovereignty, which is, according to Hardt and Negri, the “capitalist development and the affirmation of the market as the foundation of the values of social reproduction” (2000, p. 85).

It goes without saying that this is a simplification. Nevertheless, the short passage about the origins of sovereignty helps us to think about an interruption; it directs us towards a process of deterritorialization and an opening of a system of thought that soon was meat with a process of reterritorialization and the creation of modern European sovereignty, filled with a set of values of social reproduction. With hesitations about drawing a parallel between the immanent system of thought described by Hardt and Negri and the cyber-libertarian movement, I push forward, arguing that the creative desire of liberation, although, at the end, with different sentiments and objectives, lived in the spirit of what has become known as the cyber-libertarian movement. In this movement lives the utopian idea of a decentralized world without governments and without state regulations, an open and borderless world. In an essay first published in 1995 called *The Californian ideology*, Richard Barbrook and Andy Carmon describe the movement of cyber-libertarians as “bizarre fusion of the cultural bohemianism of San Francisco with the hi-tech industries of Silicon Valley” (2015, p. 12). The Californian ideology is an amalgamation of opposites, of hippies and yuppies, brought together through their profound faith in the emancipatory potential of the information technologies (Barbrook, 2015, p. 12). It is described as ambiguous ideological construction, embracing both the anti-corporate purity of the “new left” through its advocacy of the virtual community on the one hand, and a laissez-faire ideology and a right-wing conservativism, enthusiastically drawing on the new age of informatics, technologically creating a foundation for a libertarian free market, on the other side. From this soil, stems the new spirit of digital capitalism (Huberman, 2022), which is taking more market shares for each day. As a respond to digital capital extraction, as seen above, discussion about data sovereignty, data imperialism, or, colonialism (Couldry and Mejias, 2019; Chidi Oguamanam, 2020), and surveillance capitalism (Zuboff, 2019) have emerged. Another response, which also draws on a bizarre combination of an appropriation of an underdog rhetoric of digital decolonization and liberation, and, at the same time, a mercantilism on EU level, is the European digital sovereignty. This brings me to the second theme…

**References**

Adelson, N. and Mickelson, S. (2022) ‘The Miiyupimatisiiun Research Data Archives Project: putting OCAP® principles into practice’, *Digital Library Perspectives* [Preprint]. Available at: https://doi.org/10.1108/DLP-11-2021-0099.

Anderson, B.R.O. (2016) *Imagined communities : reflections on the origin and spread of nationalism.* Revised edition. Verso. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat00115a&AN=lkp.898769&lang=sv&site=eds-live&scope=site.

Balibar, É. (2004) *We, the people of Europe? : reflections on transnational citizenship.* Princeton University Press (Translation/transnation). Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat00115a&AN=lkp.381081&lang=sv&site=eds-live&scope=site.

Barbrook, R. (2015) *The internet revolution : from dot-com capitalism to cybernetic communism*. Amsterdam: Institute of Network Cultures (Network notebook).

Barrinha, A. and Christou, G. (2022) ‘Speaking sovereignty: the EU in the cyber domain’, in. *European security*, Great Britain: Taylor & Francis, pp. 356–376. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edsbl&AN=vdc.100164796926.0x000001&lang=sv&site=eds-live&scope=site.

Barry, A. and Walters, W. (2003) ‘From EURATOM to “complex systems”: technology and European government.’, *Alternatives*, 28(3), pp. 305–329.

Baur, A. (2023) ‘European Dreams of the Cloud: Imagining Innovation and Political Control’, *Geopolitics* [Preprint]. Available at: https://doi.org/10.1080/14650045.2022.2151902.

Bellanova, R., Carrapico, H. and Duez, D. (2022) ‘Digital/sovereignty and European security integration: an introduction’, *EUROPEAN SECURITY*, 31(3), pp. 337–355. Available at: https://doi.org/10.1080/09662839.2022.2101887.

Bratton, B.H. (2015) *The stack : on software and sovereignty*. MIT Press.

Brown, W. (2010) *Walled states, waning sovereignty.* Zone Books. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat00115a&AN=lkp.838964&lang=sv&site=eds-live&scope=site https://login.e.bibl.liu.se/login?url=https://ebookcentral.proquest.com/lib/linkoping-ebo.

Calzada, I. (2021) ‘Data co-operatives through data sovereignty’, *Smart Cities*, 4(3), pp. 1158–1172. Available at: https://doi.org/10.3390/smartcities4030062.

Chidi Oguamanam (2020) ‘Indigenous Peoples, Data Sovereignty, and Self-Determination: Current Realities and Imperatives’, *The African Journal of Information and Communication*, (26), pp. 1–20. Available at: https://doi.org/10.23962/10539/30360.

Couldry, N. and Mejias, U.A. (2019) *The costs of connection : how data is colonizing human life and appropriating it for capitalism.* Stanford University Press (Culture and economic life). Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cat00115a&AN=lkp.1016204&lang=sv&site=eds-live&scope=site.

Couture, S. and Toupin, S. (2019) ‘What does the notion of “sovereignty” mean when referring to the digital?’, *New Media and Society*, 21(10), pp. 2305–2322.

Csernatoni, R. (2022) ‘The EU’s hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty’, *EUROPEAN SECURITY*, 31(3), pp. 395–414. Available at: https://doi.org/10.1080/09662839.2022.2103370.

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), pp. 435–453. Available at: https://doi.org/10.1080/09662839.2022.2102896.

Glasze, G. *et al.* (2023) ‘Contested Spatialities of Digital Sovereignty’, in. *Geopolitics*, Great Britain: Taylor & Francis, pp. 919–958. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edsbl&AN=vdc.100176168555.0x000001&lang=sv&site=eds-live&scope=site.

Hardt, M. and Negri, A. (2000) *Empire.* Harvard University Press. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat00115a&AN=lkp.331033&lang=sv&site=eds-live&scope=site.

Hofmann, J. (2016) ‘Multi-stakeholderism in Internet governance: putting a fiction into practice’, in. *Journal of cyber policy*, Taylor & Francis, pp. 29–49. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edsbl&AN=vdc.100031329943.0x000001&lang=sv&site=eds-live&scope=site.

Hong, Y.( 1 ) and Goodnight, G.T.( 2 ) (2020) ‘How to think about cyber sovereignty: the case of China’, *Chinese Journal of Communication*, 13(1), pp. 8–26. Available at: https://doi.org/10.1080/17544750.2019.1687536.

Huberman, J. (2022) *The spirit of digital capitalism.* Polity Press. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat00115a&AN=lkp.1273718&lang=sv&site=eds-live&scope=site.

Hummel, P. *et al.* (2021) ‘Data sovereignty: A review.’, *Big Data & Society*, 8(1), pp. 1–17.

Jablonski, M. and Powers, S.M. (2015) *The Real Cyber War: The Political Economy of Internet Freedom (The History of Communication) [Elektronisk resurs]*. Polish American Historical Association.

Jacoby, M. *et al.* (2021) ‘An approach for Industrie 4.0-compliant and data-sovereign Digital Twins Realization of the Industrie 4.0 Asset Administration Shell with a data-sovereignty extension’, *At-Automatisierungstechnik*, 69(12), pp. 1051–1061. Available at: https://doi.org/10.1515/auto-2021-0074.

Kaloudis, M. (2022) ‘Sovereignty in the Digital Age - How Can We Measure Digital Sovereignty and Support the EU’s Action Plan?’, *New Global Studies*, 16(3), pp. 275–299. Available at: https://doi.org/10.1515/ngs-2021-0015.

Monsees, L. and Lambach, D. (2022) ‘Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity’, *EUROPEAN SECURITY*, 31(3), pp. 377–394. Available at: https://doi.org/10.1080/09662839.2022.2101883.

Mouton, M. and Burns, R. (2021) ‘(Digital) neo-colonialism in the smart city.’, *Regional Studies*, 55(12), pp. 1890–1901.

Mueller, M.L. (2020) ‘Against Sovereignty in Cyberspace.’, *International Studies Review*, 22(4), pp. 779–801.

Pericàs-Gornals, R., Mut-Puigserver, M. and Payeras-Capellà, M.M. (2022) ‘Highly private blockchain-based management system for digital COVID-19 certificates’, *International Journal of Information Security*, pp. 1–22. Available at: https://doi.org/10.1007/s10207-022-00598-3.

Pistor, K. (2020) ‘Statehood in the digital age1.’, *Constellations: An International Journal of Critical & Democratic Theory*, 27(1), pp. 3–18.

Pohle, J. and Thiel, T. (2021) ‘Digital Sovereignty’. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edsgso&AN=edsgso.76237&lang=sv&site=eds-live&scope=site.

Roberts, J.S. and Montoya, L.N. (2022) ‘Decolonisation, Global Data Law, and Indigenous Data Sovereignty’. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=edsarx&AN=edsarx.2208.04700&lang=sv&site=eds-live&scope=site.

Taylor, J. and Kukutai, T. (2016) *Indigenous data sovereignty : toward an agenda.* Australian National University Press (Research Monograph: Number 38). Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat00115a&AN=lkp.936655&lang=sv&site=eds-live&scope=site.

Zuboff, S. (2019) *The age of surveillance capitalism : the fight for a human future at the new frontier of power.* PublicAffairs. Available at: https://login.e.bibl.liu.se/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat00115a&AN=lkp.1200293&lang=sv&site=eds-live&scope=site.