

|                  |                                                                                                                                                                                                                   |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title            | Chapter 2-I : EU sovereignty in a geopoliticized digital world                                                                                                                                                    |
| Sub Title        |                                                                                                                                                                                                                   |
| Author           | Timmers, Paul                                                                                                                                                                                                     |
| Publisher        | Keio University Global Research Institute                                                                                                                                                                         |
| Publication year | 2025                                                                                                                                                                                                              |
| Jtitle           | Monsterizing Platform Power and Law ; Volume 1. Platforms and States: How to Settle the Battle of Monsters ,p.57- 71                                                                                              |
| JaLC DOI         | 10.14991/KO11003002.00000001-0057                                                                                                                                                                                 |
| Abstract         |                                                                                                                                                                                                                   |
| Notes            | Chapter 2 : The battle for the rulers of digital space                                                                                                                                                            |
| Genre            | Book                                                                                                                                                                                                              |
| URL              | <a href="https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0057">https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0057</a> |

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

# EU SOVEREIGNTY IN A GEOPOLITICIZED DIGITAL WORLD

Paul Timmers\*

---

## Introduction

Summer 2017. Something suddenly ‘clicked’ in Europe<sup>1</sup>. German *Bundeskanzlerin* Angela Merkel, stated ‘[we] must take our fate in our own hands’. She said so, just after an acrimonious NATO Summit in June 2017 where US President Donald Trump scolded the Germans for not spending enough on defense and taking advantage of the USA in areas like trade and cars. A few months later French President Emmanuel Macron gave a landmark speech at Sorbonne University. He talked about ‘une Europe souveraine, unie, démocratique’<sup>2</sup>. Sovereignty and strategic autonomy were the new words appearing in the European policy debate.

The ‘click’ or wake-up call was not only triggered by tensions in the trans-Atlantic relationship but also by rising concerns about Russia and China as growing geopolitical rivals or even adversaries. Intelligence services were ringing alarms, warning that massive cyber-theft of intellectual property was starting to put the very future of European companies and jobs at risk. Already there were uncomfortable signals that Europe was losing out in the new digital economy and society to foreign big tech. The manipulation of the 2016 US elections by Cambridge Analytica suggested that also Europe’s democracy was at risk of being hijacked by anti-democrats via social media.

---

## 1 End to naivety

From the end of the 20<sup>th</sup> century onwards, many decision-makers in Europe and the USA were subscribing to the neo-liberal vision of open markets, global competition, supply chains that could be reconfigured internationally and flexibly to minimize cost and deliver Just-In-Time. A neo-liberal global economy would maximize consumer benefits, jobs, and profits. The techno-idealism of an open, free internet was fitting very

---

\* **Paul TIMMERS:** Visiting Professor at University of Leuven; Area of Expertise: Geopolitics and Technology, paul.timmers@kuleuven.be

1 In this text, Europe and European Union or EU are used interchangeably.

2 Emmanuel Macron, “Initiative pour l’Europe - Discours d’Emmanuel Macron pour une Europe souveraine, unie, démocratique.” [elysee.fr](https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique), September 26, 2017, <https://www.elysee.fr/emmanuel-macron/2017/09/26/initiative-pour-l-europe-discours-d-emmanuel-macron-pour-une-europe-souveraine-unie-democratique>. For an analysis of the French approach in the sovereignty debate in relation to big tech see also Pauline Türk, “The State Facing Digital Giants: Competition, Collaboration And Imitation.”

well with this vision. One that would bring a better future for everyone.

However, twenty years later this vision had turned into an unsettling dream, perhaps even a nightmare of misinformation, online manipulation, digital exploitation, surveillance capitalism, weaponization of technology, and supply chain shocks. Countries felt that they were losing control over their public services, jobs, knowledge, and even the most confidential information. A bad dream in which citizens are the product, exploited as consumers and manipulated as voters. A worrying cyberspace having no viable escape exit from smart phones, social networks, and e-commerce whilst vulnerable citizens small enterprises got increasingly cornered by cyber-criminals.

When the lights were switched on and the dream ended, a concerning loss of control and autonomy became visible. The geo-politicized digital world turned out to have created an ‘sovereignty gap’<sup>3</sup> for many states and loss of strategic autonomy, that is, the means to realize sovereignty.

Even then princess Europa (to quote Greek mythology) woke up reluctantly, wanting to continue dreaming while being abducted by the Zeus of geopolitics and big tech. In 2018, a year after the wake-up calls heard by Merkel and Macron, President Jean-Claude Juncker of the European Commission, argued that it was high time to take sovereignty seriously in his State of the Union speech titled, ‘The hour of European sovereignty’. Immediately he was lambasted by half the European press: thou shalt not talk of European sovereignty! But the times are a-changin’, to quote Bob Dylan. In summer 2022, the new *Bundeskanzler* Olaf Schulz dedicated one-third of his major speech in Prague to EU sovereignty, spelling out the word explicitly. Indeed, a *Zeitenwende*.

So, the dream did end. The paralysis of the COVID-19 pandemic in 2020, explosive growth of cyber-crime, rampant misinformation and above all, Russia’s February 2022 attack on Ukraine at the very border of the EU brought the message home. Ordinary citizens, whether or not interested in war and peace, felt the massively rising energy prices. The supply chain crises following COVID-19 rubbed in the risk of dependency on others for critical materials, semiconductors, or solar panels. European leaders started to talk about ‘end to naivety’<sup>4</sup>. On top of this, the increasing loud alarm bells of climate change manifesting themselves in overheated summers and devastating floods.

Let’s summarize the factors that create this sovereignty gap: firstly, geopolitical tensions and confrontation; secondly, global threats that transcend national borders notably pandemics, climate change and cyber-crime; and thirdly, pervasive and disruptive digital transformation combined with the concentration of power in the hands of a few, foreign, big tech firms that control digital platforms, cloud and increasingly also networks and artificial intelligence.

3 Term coined by Lucas Kello, “The Virtual Weapon and International Order” (Yale University Press, 2017).

4 For instance, the Dutch prime minister in his Churchill lecture on 13 February 2019 when talking about Europe said: “The centrepiece of my message today: the importance of being less naïve and more realistic.”. In March that year, EU leaders called for an end to naivety in relations with China. European Commissioner Thierry Breton said on 11 February 2021: “[...] put an end to the era of naivety: let us take our destiny into our own hands” referring to both geopolitical, economic and technological developments.

## 2 Sovereignty in a digital and geopoliticized age

But what are we talking about when we use terms such as sovereignty and strategic autonomy? According to Karl Weick finding a word for a phenomenon and giving it a meaning, that is, sensemaking, is often triggered by a crisis. A crisis can lift a veil such that suddenly everyone is ‘seeing it’, is on one page. Indeed, the last few years we have lived a series of crises which has put new substance to these terms.

New substance, as it is about the meaning of sovereignty in this new, digital and geopoliticized age. Sovereignty thinking is, however, much older. It has evolved, at least in Europe, over the past 400 years. The beginning of the notion of sovereignty of states is often identified with the Peace of Westphalia in 1648. The Westphalian Treaties recognized states as the locus of sovereignty. They were intended to end many years of warring between kingdoms (and also involving the Catholic Church) during which probably millions of lives were lost.

In political philosophy, the notion of ‘the sovereign’ evolved from being identified with the king as the sovereign by Thomas Hobbes to the social contract and popular sovereignty as described by Enlightenment philosophers John Locke and Jean-Jacques Rousseau, which identified the sovereign as the government in a legitimized divisions of powers between citizens and the state. Winding fast-forward, another landmark moment 300 years later was the establishment of the United Nations. The UN Charter explicitly recognizes the inviolability of sovereignty of states even if it – ambiguously - also acknowledges that certain matters such as human rights transcend individual states<sup>5</sup>. Europe, like the UN triggered by World War II, saw in 1957 the establishment of the European Economic Community by 6 countries. This grew into today’s European Union of 27 countries, based on two EU Treaties and legitimized by popular democracy.

Yet, despite this history of hundreds of years, there is no consensus on the precise meaning of sovereignty and strategic autonomy *for the EU*. One reason is that the EU itself is still in the making, and, as Jean Monnet said<sup>6</sup>, advances through crises. These are at this day and age characterized by geopolitical, technological and global forces that the EU has not under control. No wonder then that the recent series of crises give new meaning to these words, to the extent that that asserting EU sovereignty is becoming essential for the EU to stay relevant for its citizens and in the world.

Let’s look somewhat closer at sovereignty and strategic autonomy in this digital and geopoliticized age, using Bickerton’s territorial-institutional-foundational framework for sovereignty<sup>7</sup>.

1) Territorial: the framework says, firstly, that sovereignty has a territorial dimension. This ‘territorial’ in a wide sense, namely concerning ‘what belongs to us’ such as physical territory, physical resources such as oil or airspace, physical assets on the land, people, culture, and values. National identity ‘is ours’. Nowadays we would add to this list also digital resources and assets such as health or genomic data, geo-

5 United Nations, “UN Charter,” United Nations (United Nations, 1945), <https://www.un.org/en/about-us/un-charter>.

6 Jean Monnet, “Mémoires - Institut Jean Monnet,” March 31, 2022, <https://institutjeanmonnet.eu/memoires-jean-monnet/>.

7 Christopher Bickerton et al., “Conflicts of Sovereignty in Contemporary Europe: A Framework of Analysis,” *Comparative European Politics* 20, no. 3 (June 1, 2022): 257–74, <https://doi.org/10.1057/s41295-022-00269-6>.

graphic data, digitized culture and cultural heritage. We can also add digital infrastructures, intellectual property etc., as far as it is owned by the state or the people.

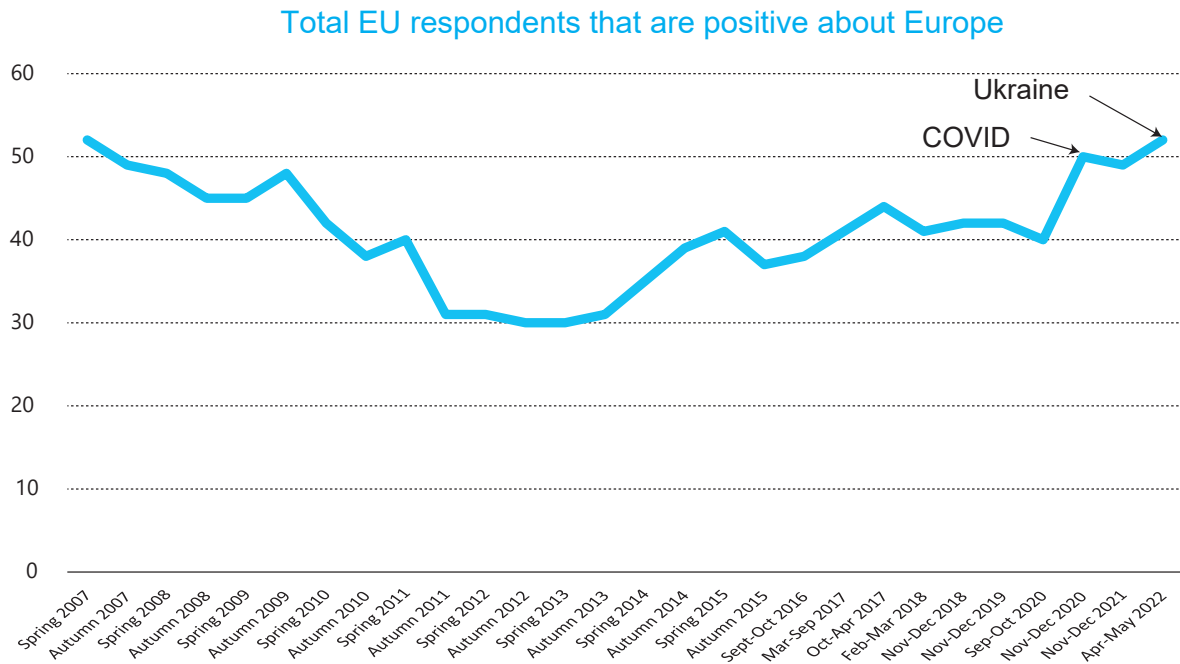
There are, however, also grey zones. Not all critical infrastructures can be said to ‘belong to us’ as after all they are largely run by the private sector which may be domestic but also foreign. The term itself, ‘belongs to us’ is ambiguous, who is ‘us’ and consequently who is ‘them’? By whom is this definition recognized or accepted, that is, in which sense is it legitimate? What does ‘belong’ mean in terms of control? Can this be moral or should it be contractual, can it be *de facto* or should it be *de jure*? These questions show that external legitimacy is a key feature of sovereignty, that is the recognition and acceptance of the state by third states.

2) Institutional: secondly, the framework distinguishes the institutional dimension of sovereignty, which is how the state is organized, in terms of executive, parliament, judiciary, and other authorities, notably where these authorities have independence under the law. In the digital age, ever more of these are digital authorities. Initially were the telecoms authority, but nowadays many countries have a data protection authority, a cybersecurity authority, a media authority, and digital competence within a competition authority. At the supra-national EU level also new regulatory authorities have been created under the EU’s Digital Markets Act and the Digital Services Act that are regulating digital platforms, while a range of supporting EU-level agencies have been put in place such as ENISA for cybersecurity. Several countries have now regular dialogues between the digitally-related authorities (an example is the UK with its Digital Regulation Cooperation Forum (DRCF)). Experts argue that it is about time to start thinking about a single digital authority<sup>8</sup>.

3) Foundational: thirdly and the most essential, is the power arrangement between government and citizens. Basic arrangements are democracy and autocracy. Foundational sovereignty shows the other key feature of sovereignty, namely internal legitimacy, which is the mutual recognition and acceptance by government and citizens of the singular power of the government and rights of citizens including in democracies that citizens are decisive in granting power to the state. The other is external legitimacy, that is, the recognition by other states of the sovereignty of the country or state. In democratic countries electoral processes such as voting or referenda must ensure internal legitimacy. In these countries, government legitimacy can always be contested, in which freedom of opinion, free press and opposition parties play indispensable roles. In autocratic countries, acceptance of internal legitimacy is *per force*, accompanied by censorship while opposition and free press tends to be suppressed. It is extensively documented how in the digital geopoliticized age internal and external legitimacy get mediated in new forms such as social media, AI algorithms, cameras and sensors, etc. offering new ways to affirm, support but also to shift and undermine foundational power arrangements, including by foreign actors pursuing their own geopolitical agendas.

---

<sup>8</sup> Georg Serentschy, Paul Timmers, and Marja Matinmikko-Blue, “Toward Anticipatory Regulation and Beyond,” in *The Changing World of Mobile Communications: 5G, 6G and the Future of Digital Services*, ed. Petri Ahokangas and Annabeth Aagaard (Cham: Springer International Publishing, 2024), 221–51, [https://doi.org/10.1007/978-3-031-33191-6\\_9](https://doi.org/10.1007/978-3-031-33191-6_9).



**Figure 1: Opinions about Europe** (source: see text)

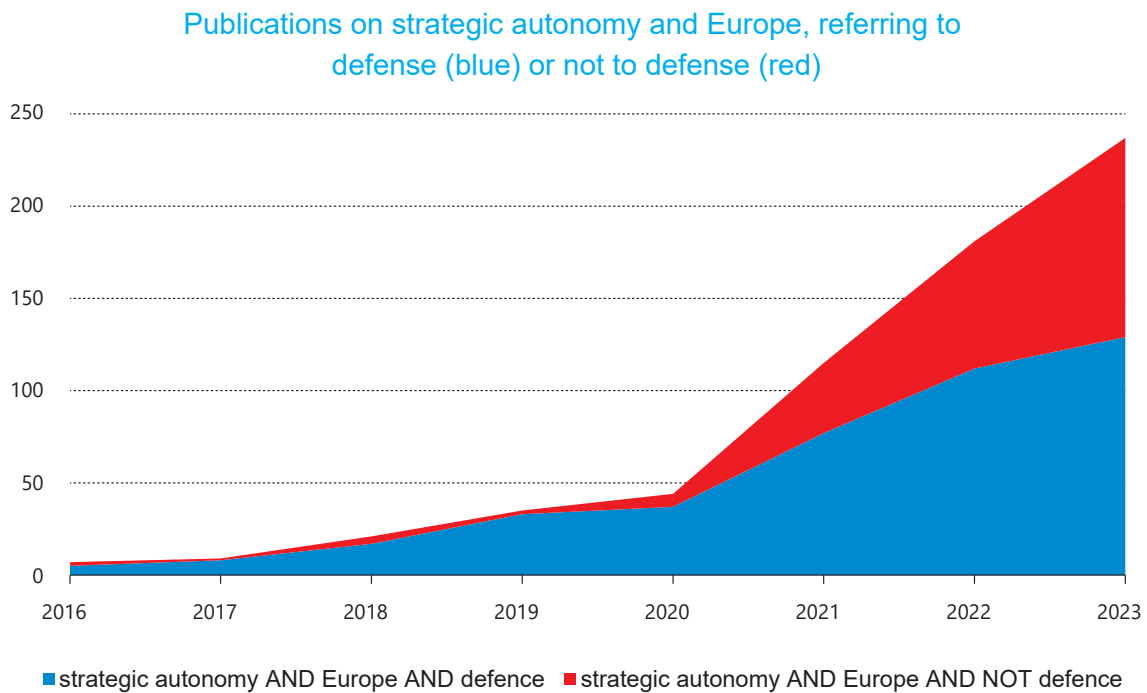
### 3 Europeans and sovereignty

How do Europeans relate to key notions of sovereignty such as ‘what belongs to us’? Surveys show that identity for Europeans closest is about family (for 81% of respondents) followed by national identity (73%) and at some distance by ‘Europe’ (56%)<sup>9</sup>. Interestingly, the appreciation of ‘Europe’, after seven meager years from 2007-2014, improved over the last seven years with marked increases during the COVID time and when the war against Ukraine started (see Figure 1)<sup>10</sup>. The COVID increase possibly was because the EU-level showed leadership in terms of organizing vaccine production and rolling out the EU-wide COVID certificate for continued free and safe travel (an international success, adopted by over 50 countries in the world). The Ukraine increase likely shows that Russia’s aggression was felt as a threat to all of the EU and not as an isolated conflict. In this crisis too, the EU-level acted firmly and jointly by welcoming Ukrainian refugees, imposing sanctions on Russia, and taking measures to soften the blow of the natural gas supply squeeze caused by the war.

Is there commonality in the discourse on sovereignty or strategic autonomy, even if there is not a unique single and commonly accepted meaning given to these notions in the EU? Academic papers retrieved by the author from Scopus in October 2023 reveal two common elements. Firstly, the number of papers addressing strategic autonomy and Europe in relation to defense has risen sharply since 2017. Secondly, the number

<sup>9</sup> Eurobarometer, “Special Eurobarometer 508: Values and Identities of EU Citizens - Data Europa EU,” November 29, 2023, <https://data.europa.eu/data/datasets/s2230-94-1-508-eng?locale=en>.

<sup>10</sup> Eurobarometer, “EP Spring 2022 Survey: Rallying around the European Flag - Democracy as Anchor Point in Times of Crisis,” 2022, <https://europa.eu/eurobarometer/surveys/detail/2792>.



**Figure 2: Academic papers on strategic autonomy**

of papers has grown even faster that are addressing strategic autonomy referring to economy, society and democracy in the wider sense, rather than to defense (see Figure 2). Moreover, a large and growing share of these are concerned with digital issues (over 40%).

The linkage to defense is obviously related to geopolitics. The growing linkage to wider economic, societal, and democracy issues and the large role of ‘digital’ in papers is suggestive though not conclusive evidence that strategic autonomy in Europe more recently is addressing a wide range of concerns across economy, society and democracy and that, next to geopolitics, big (digital) tech plays an important role in this.

## 4 Strategic autonomy

The origins of the term strategic autonomy lie with India and France. After WWII, Indian diplomacy sought to assert that it would make autonomous choices notably in defense matters, that is, independently from Washington, Beijing or Moscow. India also manifested itself as a driving force in the G77 League of Independent Nations. France, after WWII, wanted to continue to assert global presence and needed for this the atomic bomb and marine capacity such as aircraft carriers (the so-called ‘frappe de force’). These are strategic autonomy approaches from a national security perspective, expressed in military and diplomatic doctrines. Nevertheless, in particular France already at that time articulated that strategic autonomy consists in the military domain of the key elements of capabilities, capacities that should be under autonomous or

sovereign control<sup>11</sup>.

These key notions of capabilities, capacities and control (3C) can also be applied to define strategic autonomy in non-military domains such as economy, society or democracy in general<sup>12</sup>. This does not necessarily imply that there is a spillover from the military to the civil domain, although there is recently an increasing ‘securitization’ of other domains where we see the emergency of notions such as economic security. Within the societal domain, triggered by the lack of resilience during the pandemic, we also started hearing the term health security and even health sovereignty.

Is economic security a subset of national security? Surely, in the digital age the military depends extensively on commercial technologies. A strong economy is a condition to finance a strong military which international realists would say is necessary to support the external legitimacy dimension of sovereignty. It can be also argued that erosion of economic power would erode internal government legitimacy, for instance, to finance public services. Within historic materialism, as adhered to by China, economic power is the ultimate source to project national power in the world. The USA over many years has been projecting its power both economically and with its military.

For the EU, however, there is a less evident identification of economic and national security with each other. Firstly, there is no common EU-level ideological basis for this. Secondly, while a strong military requires a strong economy, this fact is hardly part of the public debate. For decades, defense matters had a relatively low profile at EU level. The EU was seen as an economic project. Matters of national security, defense included, have a very weak EU-level mandate as Article 4(2) of the Treaty on European Union states: “The Union [...] shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.”. Nowadays, due to Russia’s war against Ukraine, the need for strong military defense at EU-level is much more positive and openly expressed. Some leading military personalities are even arguing that Europe should switch to a war economy, as Russia has done<sup>13</sup>.

---

## 5 Geopolitics and big tech

Geopolitics and big tech have become closely related. Anu Bradford expounds on this in her excellent book *Digital Empires*, analyzing a ‘horizontal battle’ between states (i.e., US, China, EU) and a ‘vertical battle’ between state and big tech, as also already expressed by Prof Yamamoto<sup>14</sup>. There are complicat-

---

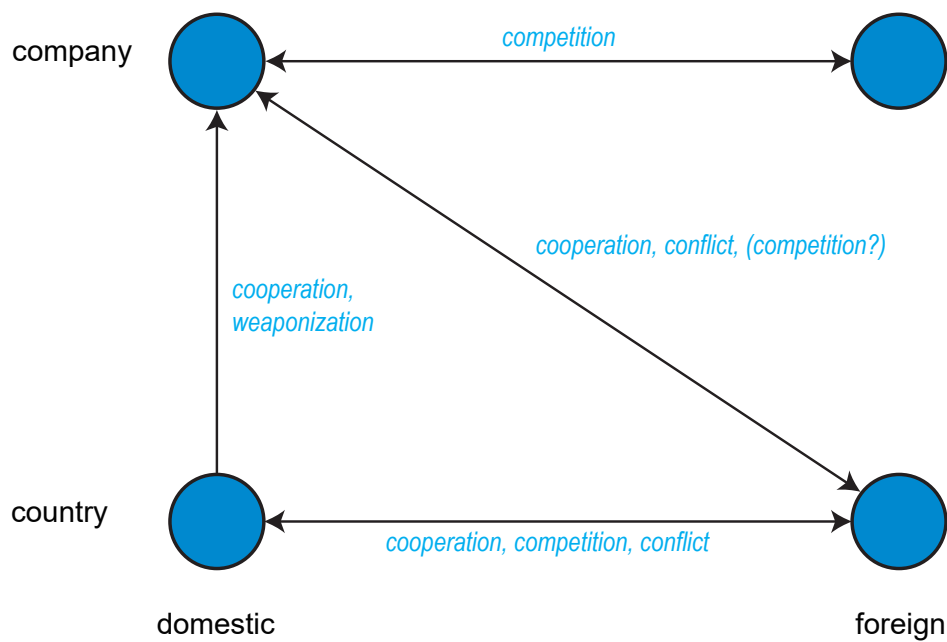
11 République Française, “Defence and National Security Strategic Review 2017,” 2017, <https://espas.secure.europarl.europa.eu/orbis/document/defence-and-national-security-strategic-review-2017>.

12 Paul Timmers and Freddy Dezeure, “Strategic Autonomy and Cybersecurity in the Netherlands | Cyber Security Council” (Cyber Security Council, 2021), <https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands>.

13 Ria Cats, “Interview Rob Bauer - De huidige onrust, ‘dat is het nieuwe normaal voor de komende vijftien jaar’ | FD,” FD.nl, November 2, 2023, <https://fd.nl/politiek/1494594/raden-van-bestuur-zien-veiligheid-niet-als-een-strategische-investering>.

14 Tatsuhiko Yamamoto, “Modern Sovereign States and Digital Platforms - Leviathans vs. Behemoths” (2023).





**Figure 3: Horizontal and vertical relations of countries and companies**

ed relations here. All three aspects, cooperation, competition, and confrontation (or conflict) play a role in combined state-state and state-company relations, i.e. in related horizontal and vertical battles. Some relations are shown in Figure 3. For instance, Farrell and Newman<sup>15</sup> coined the term weaponization of interdependencies, and exemplified this with mobilizing the international digital financial transaction system SWIFT to impose sanctions on Iran and for counter-terrorism. With its allies, that is in a horizontal cooperation, the USA has been able to control access to SWIFT and its private bank members, that is in a vertical cooperation, to exclude Iran, that is a horizontal confrontation, as well as to monitor financial transaction to detect potential international terrorist activities.

On the other hand, concerns have been raised that US big tech with its large digital platforms could exert undue pressure on the sovereignty of European countries, such as competing for control of digital identity. Big tech could also possibly be mobilized by government for foreign monitoring under the US Cloud Act or even to spy on allies as we learned from the Snowden revelations, where there are also examples where big tech seeks to resist their own government to do so. Trans-Atlantic tensions rise when the EU proposes legislation to keep big tech in check, such as the Digital Markets Act and possibly in the future, cloud security certification. We see here horizontal, vertical and diagonal battles<sup>16</sup>. The 5G Security Recommendation, which effectively has led to removing Chinese telecom equipment provider from the telecommunications networks, can be seen as the result of state-state horizontal conflict, but is also seen by some as an attempt by

<sup>15</sup> Henry Farrell and Abraham L. Newman, “Weaponized Interdependence: How Global Economic Networks Shape State Coercion,” *International Security* 44, no. 1 (July 1, 2019): 42–79, [https://doi.org/10.1162/isec\\_a\\_00351](https://doi.org/10.1162/isec_a_00351).

<sup>16</sup> In Yamamoto’s terminology both a battle between leviathans and between leviathan and behemoths.

US industry to regain ground in future (e.g., 6G) telecom equipment industry– the latter being another battle namely company-company competition. Similar concerns have been made on US semiconductor export restrictions.

Domestic-foreign relations can also include cooperation since big tech is also an ally in advancing government and economy. Firstly, to modernize government and economy in particular with digital technology. Better public services enhance the credibility of government and thereby strengthens internal legitimacy and thus sovereignty. As mentioned before, EU credibility has benefited from the COVID-19 digital certificate on which big tech cooperated with their mobile phone platforms. Secondly, in cooperation for the defense against state-sponsored cyber-attacks and or even in outright war as we see in Ukraine. This cooperation enhances the position of governments towards unfriendly foreign states and thereby strengthens sovereignty in its external dimension. The relation between government and big tech can become even so intimate that they essentially sing from the same hymn sheet and even step into each other's shoes, ideologically and in terms of their actions, a phenomenon extensively analyzed by Julie Cohen as a form of governmentalism<sup>17</sup>.

For instance, it is not exceptional that big tech tries to facilitate state-to-state cooperation and alleviate geopolitical tensions, sometimes going beyond usual private-state diplomacy. An example is Microsoft's proposal for a Digital Geneva Convention in 2017. This Convention, however, did not deliver as intended, possibly because it was ahead of its times, or possibly it was felt to get too close to the turf of governments. More recently in 2023, close cooperation between governments and companies, combined with state-to-state and company-to-company cooperation was visible at the UK-sponsored AI Safety Summit.

---

## 6 Strategic autonomy armory

Governments must protect state sovereignty and strategic autonomy is the means to do so. More specifically, strategic autonomy consists of 3C's: capabilities – what one knows to do; capacities – how much one can do; and control – having autonomy over capabilities and capacities. We need to say in which domain we have these 3C's: defense, semiconductors, cloud, batteries, vaccines, etc. These domains have to be important for sovereignty. Not having 3C's in defense would be a serious matter for most countries.

These means can be constructed along different strategies. Conceptually simplest is to fully control all capabilities and capacities, that is, to have autarky or self-sufficiency. Few countries, perhaps at most the USA and China, are able to achieve that for all domains that are critical for sovereignty. China has well-developed plans for self-sufficiency in a range of areas, amongst these the Made in China 2025 plan<sup>18</sup>. A number of digital domains are included in this plan, with priorities for instance for semiconductors and AI. Likewise the USA and the EU have lists of critical technologies for which they set out to increase strategic autonomy<sup>19</sup>.

---

17 Julie E. Cohen, *Between Truth and Power : The Legal Constructions of Informational Capitalism*, 2019; Cohen.

18 China State Council, "Made in China 2025," 2015, <http://english.www.gov.cn/2016special/madeinchina2025/>.

19 White House, "National Strategy for Critical and Emerging Technologies," October 2020; European Commission, "An EU Approach to Enhance Economic Security," Text, European Commission - European Commission, June 20, 2023, <https://ec.europa>.

Autarky is neither feasible nor desirable for most countries (if for any at all). There are three other approaches to strategic autonomy<sup>20</sup>:

1. **Risk management**, which sets out to ensure, as best as possible, to protect and defend against threats to sovereignty. This is often the approach to deal with risks, physical or cyber, to critical infrastructures (e.g., electricity, water, transport, hospitals, and telecommunications). Risk management often is complemented by insurance against residual risks. Risk management for critical infrastructures, that are largely run in many countries by the private sector, is made concrete in public policy encourages self-regulation or imposes regulatory requirements for the private sector. A typical example is market access regulation of which an example in the EU is the Network and Information Security Directive for cybersecurity of critical infrastructures. This can be complemented by guidance for government procurement. However, if the residual risk includes a serious loss of sovereignty, then there would be no way to insure against this, let alone, to get political acceptance of such public policy. Nevertheless, a risk management approach has appeal as a pragmatic, rather fast fix certainly in the past when sovereignty did not seem to be seriously threatened and when awareness of sovereignty threats was low.

2. **Strategic partnerships**, which is to cooperate with likeminded partners in order to jointly and possibly mutually strengthen sovereignty. This requires mutual trust and commitment in order to enable shared provision and control of capabilities and capacities. Such trust is based on common values such as subscribing to human rights, democracy, and liberal market economy. Strategic partnering is based on bilateral or multilateral agreements. The strategic partnership policy toolset includes industrial policy, foreign direct investment controls, export and dual-use controls, and defense partnerships such as NATO or the US-Japan Security Alliance. There is a strong trend towards strategic partnering in key technological areas such semiconductors and 5G networking. Nevertheless, strategic partnerships are both vulnerable to the winds of political change. Moreover, even together with partners self-sufficiency may be hard to achieve and must be complemented by strategic interdependency arrangements with non-likeminded parties, whether neutral ones or geopolitical opponents such that each side has more to lose than to win. Such strategic interdependencies take the form of treaties (such as for nuclear arms control) to long-term contracts such as for critical raw materials.

3. **Global common goods**, as the third approach, which means stepping out of the framing by promoting globally shared interests rather than state-centricity. A global common good approach does not impair the sovereignty of any country involved. On the contrary, it may even strengthen the sovereignty of individual states in cases where realization of benefits or countering threats far surpasses the power of countries on their own.

Global common good approaches can take the form of joint agreements and management of globally

---

[eu.commission/presscorner/detail/en/IP\\_23\\_3358](https://eu.commission/presscorner/detail/en/IP_23_3358).

<sup>20</sup> Paul Timmers, "Strategic Autonomy and Cybersecurity :: EU Cyber Direct," EUISS Research in Focus, 2019, <https://eucyberdirect.eu/research/strategic-autonomy-and-cybersecurity>.

shared assets. Examples of the former are arrangements under international law such as the International Maritime Organization for international waters or the Montreal Protocol for restoring the ozone layer or the WHO for global public health in particular to prevent or combat pandemics like COVID-19. Examples of the latter are ICANN for the management of internet domain names and precautionary-based collaboration such as enhancing the global knowledge base on climate change by the IPCC. Technology can also help to manage global common goods. Examples are distributed control enabled by blockchain for global logistics or open source software.

The policy toolset includes international agreements for cooperation (voluntary or *de jure* in the sense of international law), international standardization, and shared research. Some of the downsides of global common goods approach are that they take a long time to establish, require enlightened leadership (political, academic, civil society, business), may break down when a major participating country is willing to incur the cost of non-compliance, and that they are vulnerable to free-riders. In many areas global cooperation can be driven and even be run by the private sector, but governments will want to keep an eye on this in order to ensure that sovereignty does not get adversely affected. A particular instance where this became an issue was in 5G security, where governments got alerted late in the process of establishing 5G architecture and standards potentials perils for national security. Turning back the clock in the technology was no longer possible as 5G already was being rolled out, so fairly heavy-handed intervention had to be resorted to such as replacing 5G equipment. It remains to be seen whether standards and technology of the next-generation networks, 6G, will see the same fate or can still be managed as a trustworthy global common good<sup>21</sup>.

In the digital domain the EU pursues all three approaches. For instance, the General Data Protection Regulation (GDPR) and the first cyber-law, the Network and Information Directive (NIS1) are explicitly based on risk management. A strategic partnerships approach is pursued by the EU Chips Act where cooperation is with likeminded countries (USA, Japan, Taiwan, India<sup>22</sup>, and others). As regards global common good approach, the EU has been a strong promoter of global and multistakeholder management of internet domain names having some success opening up ICANN in this respect.

What then about the EU's policy initiatives in relation to big tech and how do these relate to the challenge to sovereignty posed by big tech? Since 2017, the EU has translated into policy action its increasing concerns about the big tech dominance in digital platforms (cloud, social media, e-commerce) and the consequences for competition (lack of level playing field, abuse of dominance, vertical integration with increasing customer lock-in). The EU also argued that more needed to be done to unlock the potential of data for EU consumers

21 Paul Timmers, "There Will Be No Global 6G Unless We Resolve Sovereignty Concerns in 5G Governance," *Nature Electronics* 2020 3:1 3, no. 1 (January 24, 2020): 10–12, <https://doi.org/10.1038/s41928-020-0366-3>; Paul Timmers and Georg Serentschy, "Sovereignty and 6G," in *The Changing World of Mobile Communications: 5G, 6G and the Future of Digital Services*, ed. Petri Ahokangas and Annabeth Aagaard (Cham: Springer International Publishing, 2024), 253–82, [https://doi.org/10.1007/978-3-031-33191-6\\_10](https://doi.org/10.1007/978-3-031-33191-6_10).

22 "Commission and India Sign Agreement on Semiconductors," Text, European Commission - European Commission, accessed November 24, 2023, [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_23\\_4380](https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4380).

and businesses as well as for the public interest. The EU's Digital Markets Act (DMA), Data Act and Data Governance Act seek to address these concerns. A regulatory implementation initiative on cloud security certification is under discussion. Industrial development impetus in the field of cloud through research, innovation and standardization is until now mainly left to Member State-driven non-legislative initiatives such as GAIA-X.

In addition, given concerns for democracy, the EU moved from voluntary, self-regulatory approaches by the big content platforms as regards harmful and illegal content and disinformation on their social networks to a much stricter regulatory approach in the Digital Services Act that entered into force in 2022 and started to be applied in 2023.

Most recently, the EU is putting in place an economic security policy, that seeks to reduce dependencies on third countries in selected critical technologies, such as AI, quantum technologies, advanced semiconductors and biotechnologies<sup>23</sup>. This policy states that it seeks 'to make the European economy and industry more competitive and resilient and strengthen our open strategic autonomy'. It also states four areas of concern: (1) resilience of supply chains; (2) physical and cyber security of critical infrastructure; (3) technology security and technology leakage; and (4) weaponisation of economic dependencies or economic coercion. However, it is not in a direct way addressing big tech. Rather it focuses on state-to-state relations, as they impact supply chains, critical infrastructures, and knowledge base.

The EU Economic Security policy should also be read in conjunction with the EU Chips Act and the EU Critical Raw Materials policy. Both are a mix of market access regulation and industrial policy. They seek reducing dependencies that can disrupt resiliency and business continuity but also – in the long run – erode sovereignty. They contain support for building up domestic capacity and engaging in new partnerships with 'friendly' countries. Increasingly these become 'geopolitically-aware industrial policies'<sup>24</sup>. They are, however, not (yet) fully comprehensive as they would then have to be extended further into combining investment, public procurement, standardization and market access regulation, as well as have an even more extensive and pro-active international dimension in order to anticipate geopolitical reactions such as subsidy races and retaliatory export controls as we start to see in the field of semiconductors and raw materials.

It is tempting to interpret these regulatory and non-regulatory initiatives as flat-out attempts by the EU to increase strategic autonomy and thereby regain a degree of sovereignty. However, it is hard to argue this from public evidence only. Often these policy initiatives are not explicitly or not extensively phrased in terms of sovereignty or strategic autonomy. For instance, one of the most groundbreaking initiatives, the DMA mentioned above, does not refer to these notions at all. Yet, many of these initiatives do refer to improving Europe's competitiveness and express worries that loss of competitiveness would also affect Europe's position

23 European Commission, "An EU Approach to Enhance Economic Security"; European Commission, "Commission Recommends Carrying out Risk Assessments on Four Critical Technology Areas: Advanced Semiconductors, Artificial Intelligence, Quantum, Biotechnologies | Shaping Europe's Digital Future," October 3, 2023, <https://digital-strategy.ec.europa.eu/en/news/commission-recommends-carrying-out-risk-assessments-four-critical-technology-areas-advanced>.

24 Paul Timmers, "Digital Industrial Policy for Europe | CERRE Report" (CERRE, December 12, 2022), <https://cerre.eu/publications/digital-industrial-policy-for-europe/>.

in the world in a broader sense. At the political level also wording is used that calls for stronger European industry<sup>25</sup> referring to competition with foreign big tech<sup>26</sup>.

A more balanced interpretation is that these initiatives are based on a combination of concerns: resilience, competitiveness, consumer interest, democracy, values, and sovereignty. They also combine directly and indirectly state-to-state and state-to-company policy actions. In these combinations the weight of sovereignty/strategic autonomy has significantly increased over the past years, but it is not the sole and often not even the dominant argument. Protectionist and ‘European champion’ intentions may sometimes play a role but this is far from a dominant or decisive voice<sup>27</sup>.

---

## Conclusion: there is no choice

The EU is often presented as a regulatory power, but nevertheless appears to continue losing economic strength. Liberal democracy and human rights that are foundational to the EU, get ever more eroded across the globe. The EU is very concerned about geopolitical conflict, tangibly brought home by a devastating war right at its border. Internal divisions continue to distract EU decision-making even threaten to create a swing to populism and anti-EU-ism. All of this is putting EU autonomy, EU sovereignty, under much pressure. The EU has no choice but to strengthen the defense of its sovereignty, that is, to strengthen its strategic autonomy as the alternative would be erosion of the EU and losing more control over the own future, in terms of jobs, education, democracy, and values.

Is the evidence for this thesis conclusive? It is impossible to be fully affirmative as this amounts to knowing the future. Is this evidence strong for EU digital strategic autonomy? Probably we have to say, yes, it is. For instance, in semiconductors the EU’s market share has shrunk from 20% to 8%. In cloud the dominance of foreign providers (mostly US) has grown over the past 3 years from 65% to 75% of market share. The EU is for a range of critical raw and processed materials for 90-100%, dependent on China. In solar panels, once leading, the EU has massively lost market share to China, and the same threatens to happen in wind turbines.

The EU is not passive and is taking action with policies for economic security and critical technologies, digital market regulation, industrial policy, R&D investment and joint funding of IPCEIs<sup>28</sup>, antitrust decisions, state support and anti-dumping investigations, international deals, etc. There are rays of hope for the EU: in supercomputers the EU was absent from the top-20 in 2016. It has regained in 2023 two of the top-10 places. In batteries for electrical vehicles in the next few years the EU will be able to meet two-thirds of its demand through home-grown production. The EU has dramatically increased the speed of its deci-

25 Thierry Breton, “Neither Autarchy nor Dependence – More European Autonomy | LinkedIn,” August 25, 2022, <https://www.linkedin.com/pulse/neither-autarchy-nor-dependence-more-european-autonomy-thierry-breton/>.

26 Laura Kayali and Florian Eder, “Thierry Breton ‘Understands’ Trump on TikTok, Wants Data Stored in Europe,” POLITICO, September 1, 2020, <https://www.politico.eu/article/breton-wants-tiktok-data-to-stay-in-europe/>.

27 Even ‘European champions’ tend to be anchored in a few EU countries only, reflecting persistent national voice.

28 IPCEIs are Important Projects of Common European Interest.

sion-making. For instance, revised cybersecurity legislation was decided in just a little more than one year, whereas the first cyberlaw (NIS Directive) took several years to get adopted. Decision-making at EU level has also entered into what previously seemed to be no-go territory, and successfully so. Over the past few years there was joint EU-level decision-making on public health to combat the COVID-19 pandemic, despite the fact that health is seen as a national prerogative. Similarly for matters that are very close to national security – where the EU formally has no mandate –, namely defense and certain aspects of cybersecurity. Moreover, the taboo of shared debt at EU-level has been broken by establishing a large pandemic recovery fund.

Are these policy initiatives still in time and provide a sufficient and effective set of actions? Will future strategic autonomy-building policy still fall on such fertile ground as was the case in recent years? Europe is divided. An active nationalist populist movement is gaining ground, some with authoritarian inclinations and dubious ties to Russia and China. Such parties once in power could actively undermine the EU. They present the relation between national and EU sovereignty as a win-lose proposition. They do not stress an EU of values but rather an EU of national ‘sovereign’ states.

Paradoxically, by stressing national sovereignty and undermining EU collaboration, populist and nationalistic movements may well be endangering rather than rescuing national sovereignty. The forces of geopolitics, big tech and planetary challenges are much greater than the power of an individual (EU) country. There are vast areas, such as in the world of digital, where it can be argued that EU-level cooperation, rather than a win-lose, is a triple win. Namely, a first win is that joining up gives enough critical mass to counter digital threats to sovereignty at the national level. A second win is that doing so enriches shared sovereign digital assets such as dataspace, digital identity, interconnected, interoperable digital networks and services, and a digital topography such as the domain name system of .eu and Member States’ country-level domains. The third win is that by working together as EU Member States, the EU has a stronger position in the world to take part in negotiations on international governance, regulation, standards, and trans-national digital solutions<sup>29</sup>.

In these conclusions, a few words of warning, though. Firstly, we do not argue to promote sovereignty in an indiscriminate way. Sovereignty is a word readily used by authoritarians and populists. It is therefore very important to qualify that sovereignty is used here is within the wider commitment to promote liberal democracy, fundamental rights and broader interests for the planet.

Secondly, it is hard to detect at EU-level ‘hegemonic intent’ in the sense of an intent to dominate others in the world. The way nowadays the EU interacts with the world is not comparable to the approach of past empires. Anu Bradford, despite discussing the EU as a regulatory digital empire<sup>30</sup> also does not argue that the EU exercises regulatory imperialism but rather that there is a dynamics at work, the ‘Brussels Effect’, that creates both *de facto* and *de jure* adoption in other countries of approaches that are compatible with EU

29 Paul Timmers, “When Sovereignty Leads and Cyber Law Follows,” October 13, 2020, <https://directionsblog.eu/when-sovereignty-leads-and-cyber-law-follows/>.

30 Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (New York, NY: Oxford University Press, 2023).



regulations. Imperialistic thinking is not part of the European project or part of the quest for EU sovereignty.

Thirdly, as shown above, there are significant and justified concerns about the concentration of power with big digital tech. There is reason to be concerned for democracy, national security and future autonomy over economy and jobs. EU sovereignty is at stake in a world dominated by foreign big tech. But that does not imply that the EU's reaction is or should be to wage a battle against big tech, let alone to consider this a hegemonic battle. Rather, EU's policy actions should also address safeguarding sovereignty in a geopolitical digital world and balance cooperation, competition and confrontation. Further research has to assess whether this balance does strengthen EU sovereignty.

Finally, and most importantly the discourse on EU sovereignty, whether in relation to big tech or geopolitics, is part of a long historic discourse on European identity. Driving forward this quest is determining, even existential, for the future of the EU.