

Dóra Molnár

DIGITAL SOVEREIGNTY OF THE EUROPEAN UNION

PAST, PRESENT OR IS IT THE FUTURE?

INTRODUCTION

European Strategic Autonomy was first used in the context of the security and defence of the European Union and was not explicitly defined until the European Union (EU) adopted the EU Global Strategy of 2016, when it was given a broader strategic ambition.¹ Since then, successive events and developments have made strategic autonomy even more attractive and timely. Suffice it to think of the Covid-19 pandemic, concerns about the changing role of the United States in international politics, transatlantic and transpacific tensions in international trade, or the recognition of China as a strategic challenge rival, exacerbated by concerns about its dominance in the world's digital markets. These events, coupled with the EU's recognition that its own smart digitalisation is a prerequisite for the EU's strategic independence, alongside its industrial, energy, defence and sustainability policies, have led to the emergence of European initiatives to strengthen Europe's position as an independent actor and its status and role in world politics and the global economy. The framework for these is called the European Digital Strategic Autonomy (DSA) (STOLWIJK 2022).

The concept of strategic autonomy was incorporated into the political discourse by French President Emmanuel Macron in 2017, following his election, and the terms digital autonomy, digital sovereignty and technological sovereignty have subsequently come to occupy a prominent place in both political discourse and policy documents.

Being autonomous means being able to achieve our key strategic goals free of external influence and dependencies. Achieving digital autonomy in the European

¹ The EU's 2016 Global Strategy puts the security of the Union at the top of its priorities. In this context, it specifically emphasises the strengthening of the Union's strategic autonomy and its role as a security community. This is not without reason, as this is one year after the start of an unprecedented wave of migration, which has had an impact on the European Union the like of which European states have never seen before. On the new features of the migration wave see VECSEY 2019.

Union therefore depends on creating an environment in which we can sufficiently and necessarily exclude technologies and competitive pressures from global competitors, notably from the United States of America (U.S.) and China. However, technological dependency has several dimensions that need to be taken into account in order to achieve digital sovereignty, since, in addition to technical issues, economic, legal, political or even military interference can be an obstacle to the creation of an independent and competitive European digital market, and the two major powers have no interest in supporting the EU's digital autonomy ambitions, thereby strengthening a potential competitor.

Two major triggers can be identified that have significantly boosted the EU's drive for digital sovereignty, especially in recent times. The first is the changing geopolitical landscape² and the emergence of new rules on data control (STOLWIJK 2022), while the second concerns the series of legal actions against major tech companies (Google, Apple, Facebook, Amazon, Microsoft – or GAFAM), which represent a specific direction for EU legislation (THIEULIN 2019). Against this background, the paper first presents the changing geopolitical landscape, with a particular focus on the actions of the United States and China,³ which are crucial for the EU's ability to achieve digital autonomy, and then outlines the concrete steps the EU has taken in the main areas that can be considered the first milestones on the road to digital autonomy.

“GREAT POWERS” OF CYBERSPACE

Cyberspace, one of the most topical sites of geopolitical struggles, is one of the best historical examples of the emergence of digital dependency. While traditional physical dimensions have been the site of intense competition between great powers throughout history, it is only in the last 30 years that digital technologies and the networks they create have emerged on a large scale and radically reshaped our world. Moreover, unlike physical space, which is mostly shaped by nature, cyberspace is a virtual space created entirely by humanity, and more specifically by the United States of America, which would not exist without the help of excellent scientists and U.S. government funding. Moreover, cyberspace does not easily identify classical

² In this context, we merely refer to developments such as the characteristic features of the multipolar world order, the rise of the Indo-Pacific region and the role of developing countries, and the emergence of China in particular on the world stage.

³ On cybersecurity and cyber diplomacy efforts by great powers see D. MOLNÁR 2022.

resources that could justify the special attention that this intangible site receives in the world political arena.

The major powers playing a dominant role in cyberspace are nowadays well defined around the trio of the United States, China and the European Union, which are actively shaping cyberspace processes and leading the way in related economic investment, and research and development. However, this was not always the case.⁴

With the end of the bipolar world order and the dawn of the global expansion of Pax Americana, few imagined that digital space would one day be the defining issue of world politics. But the U.S. Government's policies at the time foresaw the internet as a tool for global dominance. Already one of the early but perhaps most important strategies of Bill Clinton's first presidency, *The National Information Infrastructure: Agenda for Action (NII)*, published in 1993, set out the following:

"Information is one of the nation's most critical economic resources, for both the service and manufacturing industries, the economy and national security. According to an estimate, two-thirds of U.S. workers are employed in information-related jobs, and the rest in industries that rely heavily on information" (BROWN 1993: 2).

Not only did this make it clear thirty years ago that information is a power that is fought for, possessed and used in the same way as any other resource, but also that the American economy was already built around information.

It is interesting to note that while in the early 1990s Japan seemed to be the most competitive rival to the U.S. (and partly to the EU) in this field, China is now clearly the obvious second, and in some areas the first, country in the technology field. For a country that was economically insignificant in the early 1990s, China's ability to build the advanced digital economy that Europe could have done is extraordinary. Paradoxically, the global opening of the Pax Americana helped a lot. Chinese students turned up en masse at the best universities in the U.S., while U.S. and European manufacturers opened manufacturing plants in China in the hope of cheap labour. Ostensibly, it was all about the U.S. economic advantage, as the brain drain strengthened the U.S. knowledge-intensive economy, while the resulting products could be produced as cheaply as possible in Asia. In the 2000s, however, Chinese engineers and scientists began to return home and put their knowledge to work in Chinese universities and companies. Intellectual property that was taken over by China in the manufacturing process was treated rather loosely by the locals,

⁴ The study focuses only on the state level and does not address the role of the private sector in cybersecurity. It also avoids examining and analysing the behaviour of 'rogue states' (such as Iran or North Korea) in cyberspace and its geopolitical implications.

who copied Western solutions in a way that even bordered on industrial espionage. It is no wonder that, by the 2010s, the intellectual capital and manufacturing capacity to create digital capabilities had been created (ZHANG–ZHOU 2015: xiv–xix). By contrast, European students stayed on after their U.S. studies, young engineers from European universities were lured away in droves by U.S. companies, and the best European academics received substantial grants to continue their research in the U.S.

The third major player in cyberspace is the European Union. The *Bangemann Report* is considered to be the first document that laid the foundations for digital development and the information society in the EU. It was published in May 1994, setting out the path that the European Commission would follow with minor adjustments over the following decades. Three decades later, it is interesting to note the philosophical differences between the American and European visions, which have led to Europe's long-term digital dependence.

First, the document already states in its executive summary that the EU is at a competitive disadvantage (European Commission 1995: 3). This is particularly thought-provoking today, in 2024, as the competitive disadvantage looks set to increase. On the other hand, it sees the key to closing the gap in promoting an entrepreneurial mentality and creating common rules, without the need to allocate additional financial resources (European Commission 1995: 3). Thirdly, it adds that “the current European technology base is sufficient to allow the applications proposed in this report to be deployed without delay” (European Commission 1995: 22) – meaning that no further developments are needed at present, and that they may be needed in the near (or distant) future at the most. I think that the difference in approach between the U.S. and EU documents, which were produced almost simultaneously, is quite obvious. While the ideas in the Agenda (NII) foresaw that the powers competing with the U.S. should be able to offer an alternative and develop their own capabilities in the field of information technology, and this was already known at the time of the Bangemann Report, European policy did not recognise that regulation and market liberalisation alone would not make the region competitive with the U.S. (and later Chinese) competitors in the long term.

The evolution of the U.S.–China–EU triangle

Out of the three geopolitical actors, China is clearly the one that has taken the least expected path over the last thirty years, and even the last 10–15 years. This is above all due to the push for public investment in the digital industry. The 12th Five-Year Plan adopted in 2012 already explicitly supported the strengthening of

the manufacturing capabilities of emerging technologies, and the 13th Five-Year Plan in 2017 put a strong emphasis on the diffusion of technologies such as mobile technology, cloud computing or the Internet of Things. Furthermore, the China 2025 strategy makes it clear that China's goal is to become the strongest "cyber power" (GODEMENT 2018). Again, the fact that the same orientations could only be found years later in the EU strategy documents (see in more detail the previous section) is an indication of the European backlog, and it is also a fact that closing the gap of at least a decade will require an enormous increase in budgetary resources from European Member States, which may not be a priority in wartime, and political obstacles also have to be taken into account. The U.S. has already recognised the emerging Chinese threat in the technological field during the Obama Presidency and has started to block China's activities in this area. During the Trump Presidency, for example, it has used tough sanctions to discourage the entry of Chinese technology companies, from banning 5G technologies and blocking some Chinese mobile phone manufacturers from using U.S. software to attempting to buy up one of the most popular Chinese-owned social networks. Under President Biden, this trend is deliberately continuing, with China as the primary strategic adversary for the U.S., and it is trying its best to maintain its global position and break China's emergence as a (cyber)power. The EU Member States are rather divided on these issues, for example the ban on Chinese 5G technology has only been achieved in the most loyal U.S. allies, despite the presence of major European 5G manufacturers, and this move could contribute to the development and sovereignty of the European digital industry, while reducing the potential national security threat. However, instead of a unified European policy response, in this case too, only one regulatory step, the creation of an EU toolkit on 5G Cybersecurity, has been taken, postponing the solution to the problem for years.

Meanwhile, the relationship between the two great powers, the U.S. and China, includes a number of issues that will leave open the question of cyberspace dominance in the coming decades and will massively influence the EU's moves towards digital autonomy. Perhaps the most important of these is how the post-World War II global policy of multilateralism and international organisations will evolve. Russia's military aggression against Ukraine and the annexation of sovereign Ukrainian territories by a member of the UN Security Council will clearly shake up the international order, upset the status quo and could reinforce China's intentions to shape the international order in line with the 21st century balance of power, including a national shift of global (U.S.-dominated) cyberspace towards nationalism, helping to create national networks (splinternets). Europe is not interested in this and supports the maintenance of the current cyberspace in all international fora, but this seems to

be creating an East–West confrontation on digital technology issues, in which it is very difficult to defend European interests.

Another important question is China's intentions towards Russia and Taiwan. Russia's belligerent aggression is punished by the Western world with heavy technological sanctions, so if Russia wants to keep its economy in the 21st century, it has only China to work with. In cyberspace, Russia has been fighting U.S. dominance for decades and exploiting the leverage of technology to achieve its own ends, but its belligerence will cut it off from these opportunities for a longer period, both diplomatically and technically. In cyber diplomacy, however, it has typically moved together with China, so it is likely that intentions will not change, but will be articulated by China in the future, primarily in accordance with its own interests. Thus, Russia will most probably lose its position as a cyber power and become dependent on China, but a united European stance, for example in the area of technological sanctions, is likely to provoke countermeasures on the Russian side. So, it is not enough that the EU's digital industry will lose a significant market, but it can also expect hostile action from Russia in the form of cyberattacks.

THE EVOLUTION OF THE EUROPEAN UNION POLICY

The need for regulation was already recognised by the European Union in the mid-2000s and it started to build its cybersecurity framework. As the EU approaches many threats primarily from a civilian perspective, including threats in cyberspace, its focus is on creating a free and open internet, primarily through greater international cooperation and the development of regulatory frameworks.⁵

Creating the framework for digital sovereignty – The 2010s

The highest level of regulation concerns the strategic level. In December 2003, the EU adopted its first security strategy entitled “European Security Strategy. A Secure Europe in a Better World” (Council of the European Union 2003). The document lists the global and specific challenges facing Europe, which do not include cyber threats by name, but already refers to critical infrastructure by highlighting international terrorism and the vulnerability of societies. A milestone in the long process of reviewing the strategy was the report published in December 2008, which already

⁵ For a summary table of EU strategy papers see A. MOLNÁR 2022: 46.

identified cybersecurity as a key challenge. The report refers to the high dependency of modern societies on critical infrastructure, including the world of the Internet. The need to revise the 2003 strategy has become increasingly urgent due to the rapid and dramatic changes in the global environment. The dependence of states on digital technologies has increased dramatically and it has become a strategic interest for the EU to ensure that its citizens have access to secure internet for all. The process of developing the strategy has been slow and it took the European Union around 13 years to adopt the new document. The EU's new security strategy entitled "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy" (European External Action Service 2016), already includes cyberspace as a named and prominent one among the instruments and policies to address the challenges.⁶

The first document specifically addressing the protection of information systems was issued by the EU in 2009: the Commission Communication "Protecting Europe from Large Scale Cyberattacks and Disruptions: Enhancing Preparedness, Security and Resilience" (European Commission 2009). Among the shortcomings, the document highlights that cyber defence exercises at EU level are still at an embryonic stage and that multi-country exercises are rare. It therefore stresses the importance of cooperation with other organisations with established practices in this field, notably the UN, NATO, OECD and G8. A forward-looking finding of the Communication was the need to establish national cyber disaster response teams, with adequate capabilities in both early warning and incident management. The 2009 Communication was revised in 2013. In its report (European Commission 2013a) the Commission Working Group had already separated critical infrastructure protection activities into the three categories of prevention–preparedness–consequence management. It set a deadline of the second half of 2014 for the implementation of the initial objectives.

EU cyber legislation was given a new impetus by the launch in 2010 of a ten-year program called the European Digital Agenda (European Commission 2010), which focused on making cyberspace safe and secure. In 2012, the European Parliament adopted a resolution entitled "Critical Information Infrastructure Protection: Towards Global Cyber-Security" (European Parliament 2011). Although the document could not bind Member States, it set out proposals that were actually implemented in EU countries by the end of 2010. These included the creation of a national cybersecurity strategy, cyber emergency planning, the establishment of a standalone cyber defence organisation and the creation of national legislation,

⁶ For a more detailed analysis of the strategy see MOLNÁR 2016.

all of which are building blocks for digital sovereignty. The EU cybersecurity strategy was only a step from there and was put in place the following year. In 2013, the EU published its first comprehensive cybersecurity strategy, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace” (European Commission 2013b). The strategy has made it a top priority to develop the capabilities to prevent, detect and respond to cyberattacks, to reduce cybercrime sharply, to develop an autonomous cyber defence policy and capabilities within the EU’s common security and defence policy, to create the necessary industrial and technological capacities and conditions, and to establish an autonomous EU-level cyber policy as a policy along the lines of the EU’s core values. These priorities have set the organisation ambitious goals, the achievement of which is still ongoing today. However, the strategy only addresses the issues of preventing and responding to the failure or any attacks on European infocommunications systems, leaving unanswered questions such as how the European Union as a whole should respond to a cyberattack on one of its Member States under the Lisbon Treaty clause.

The adoption of the “European Digital Single Market Strategy” in 2015, a very important document for the digital sovereignty of the European Union, set the goal of creating a Digital Single Market for Europe. Its benefits were already recognised by the legislators at the time, including the potential for a significant increase in European GDP⁷ and the creation of new jobs. As regards the former, they already highlighted the booming performance of the big data sector, with an annual growth rate of 40%, seven times faster than the annual growth rate of the IT market.

The latter finding also foreshadowed a new direction for EU legislation to give the EU a competitive edge in an increasingly data-driven economy. After a long consultation process lasting around four years, two landmark pieces of legislation were adopted in 2016: the NIS Directive (Directive on Security of Network and Information Systems) and the General Data Protection Regulation (GDPR). In 2018, these were followed by the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union (European Parliament 2018), and in 2019 by the Directive on Open Data and the Re-Use of Public Sector Information (European Parliament 2019). The Data Governance Act (European Parliament 2022) completed the EU’s data protection legislation in 2022, thus completing the EU’s data protection regulation.⁸

⁷ The creation of a European Digital Single Market was then projected to lead to an increase in EU GDP of €415 billion.

⁸ Meanwhile, the EU has also been building the institutional backbone for cybersecurity over the years, which is not covered in this paper. For more on this see KASPER et al. 2021: 7.

*Where does the European Union stand now?
Developments in the 2020s*

The European Union's objective for the coming years and decades, the so-called *European Digital Strategic Autonomy* (DSA), is characterised by, among other things, long-term thinking, the innovation orientation, the knowledge base, the building of a strong consensus framework with partners and allies, the review of telecoms market regulation and the establishment of a strong regulatory framework for data protection, privacy and network security (POGOREL et al. 2022: xi–xii). DSA also represents a delicate balance of power with China. Given the interdependence between Europe and China, the EU wants to establish a clear policy framework that can react quickly to developments and monitor in real time the evolution of the relationship and its impact.

At the beginning of the decade, in 2020, the EU took an important step by adopting a new cybersecurity strategy. Adopted on 16 December 2020, the document entitled “The EU's Cybersecurity Strategy for the Digital Decade” (European Commission 2020a) focuses specifically on the framework and opportunities for the EU to build its strategic digital autonomy. It explores how the EU can harness and further increase its resources to become technologically sovereign and makes concrete proposals for the use of three main instruments: regulatory, investment and policy initiatives. To do so, it encourages the EU to act in three areas: 1. resilience, technological sovereignty and leadership; 2. building operational capacity to prevent, deter and respond; and 3. advancing a global and open cyberspace. It is therefore evident that the Union's technological sovereignty is based on the resilience of all services and products, but also on the need to increase cooperation and build additional capacity. When these findings are compared with the Bangemann Report of 1994, there is reason for optimism about the change in the EU narrative and the willingness of the organisation to go further to achieve the desired results, not being satisfied with what has already been achieved.

The European Union's initial misguided vision of a direct public support system is to be corrected by another document: the “Digital Decade for Europe: Objectives for 2030”, adopted on 9 March 2021. The document, called the Digital Compass, sets out the objectives for Europe's successful digital transformation and highlights Europe's ambition to achieve digital sovereignty:

“The EU's ambition is to be digitally sovereign in an open and interconnected world, and to pursue digital policies that empower people and businesses to seize a human centred, sustainable and more prosperous digital future. This includes addressing

vulnerabilities and dependencies as well as accelerating investment” (European Commission 2021a).

This is a significant step forward from the approach of previous decades and recognises the need for strategic European investment in digital technologies. The program sets different targets in four areas: training digitally literate citizens and highly skilled digital professionals, building secure, efficient and sustainable digital infrastructures, digital transformation of businesses and digitisation of public services (European Commission 2021c).

It is no coincidence that education and training are the top priority, as they are the be-all and end-all of Europe’s digital autonomy. The issue needs to be approached from two perspectives. On the one hand, there is a need to ensure that the concept of cybersecurity education provides the necessary level of knowledge and operational practices and, on the other hand, to train enough skilled workers to meet the needs of the cybersecurity sector and all sectors that need to interface with and apply cybersecurity services and solutions (European Organisation for Security 2019). Recognising this, several EU initiatives have already been taken to boost digital workforce skills. These include the Digital Skills and Jobs Coalition already established in 2016 or the Blueprint for Sectorial Cooperation to identify skills gaps.

Although the Compass sets out objectives and targets, it lacks clearly integrated and coherent policy measures and there are inconsistencies between objectives and targets. To partially address these gaps, on 15 September 2021, the European Commission presented its policy program “Roadmap to the Digital Decade”, which aims at complementing, completing and implementing the vision, objectives and actions of the Digital Compass. With the new program, the Commission proposes an annual cooperation mechanism with Member States consisting of four elements to support them in achieving the 2030 targets: 1. a transparent monitoring system based on an enhanced Digital Economy and Society Index (DESI) to measure progress towards the targets; 2. an annual “State of the Digital Decade” report to assess progress and make recommendations; 3. multi-annual strategic roadmaps for each Member State; and 4. a mechanism to support the implementation of multi-country projects.

The Digital Compass (European Commission 2021b) therefore defines cybersecurity as a key element of the EU’s technological sovereignty. In contrast, the Strategic Compass (Council of the European Union 2022: 3), takes a different approach, analysing and assessing cybersecurity in a purely geostrategic context. It clearly states that the EU must deepen partnerships which are in favour of EU values and interests, however, a more tailored and integrated approach to capacity

building is needed, including the need to find the links between military assistance and civilian capacity building, governance, security sector reform, and the capacity to respond to cyberattacks, disinformation and hybrid threats (Council of the European Union 2022: 44).

Defining the latest direction on regulatory issues is clearly necessary to preserve the EU's digital sovereignty in the future. In 2022, the EU adopted two major regulations: the Digital Services Act (DSA) and the Digital Markets Act (DMA). While the former aims at protecting the digital space against illegal content and guaranteeing the protection of users' fundamental rights (the guiding principle being that "what is illegal offline must be illegal online"), the DMA primarily regulates the role of the so-called "gatekeepers", as its main aim is to create a single regulatory framework for digital markets. In this way, it can help economically dependent European companies to enter the market, stimulate innovation and create a free shopping environment for consumers by ensuring quality, fair and competitive prices for digital goods and services.

Finally, as a concluding thought on regulatory issues, the evolution of the regulatory environment for AI should be mentioned. The White Paper on Artificial Intelligence, published back in 2020, was a forward-looking initiative at the time. By today, the EU has already adopted the so-called AI Act (European Parliament 2024) which, at a time when this technology is now being called the 5th Industrial Revolution, is crucial for the EU to remain a viable and competitive player among the technological superpowers.

THE RANGE OF PRACTICAL PROBLEMS

The framework outlined in the previous section is only the theoretical side of the issue, and the major question is how and how successfully it can be translated into practice. Obstacles may arise not only from the Union's bureaucratic system, but also from the creation of financial resources. The European Investment Bank estimates the EU's investment gap to achieve the potential benefits of digital transformation at €65 billion per year (European Investment Bank 2016: 33). Moreover, the Commission estimates that Europe's investment gap in digital transformation with the U.S. and China stands at €125 billion per year (European Commission 2020b: 18). Nevertheless, the EU could not only gain political and strategic capital from these investments, but also expect a significant economic boost, as the cumulative GDP contribution of new digital technologies could reach €2.2 trillion, a very significant increase of 14% compared to the base year 2017 (European Commission 2020c).

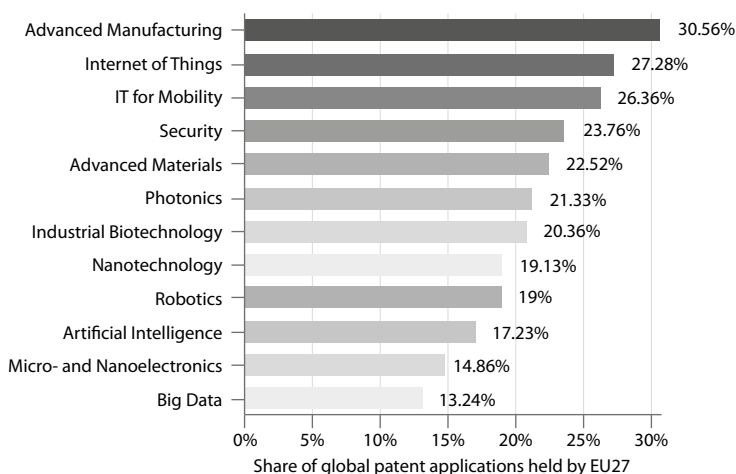


Figure 1. *Strengths and weaknesses of the 27 EU Member States in the production of advanced technologies in 2021*
Source: European Commission 2021d

The European Commission's Advanced Industrial Technologies project (European Commission 2021a) tracks technologies considered to be of strategic importance for the future. These include advanced manufacturing, artificial intelligence, big data, cloud services, industrial biotechnology, Internet of Things (IoT), micro- and nanoelectronics including semiconductors, nanotechnology, robotics and cybersecurity, among others. Keeping up with technological progress is also a sine qua non for the EU to achieve digital sovereignty and should therefore be a priority for the EU in all segments.

Figure 1 on the current performance of the EU shows how the EU's performance varies across technologies: it has performed exceptionally well in advanced manufacturing, while it also performs well in the categories of Internet of Things, mobility and security. However, there is a huge gap in four areas that are also key to achieving digital autonomy: big data, micro- and nanoelectronics, artificial intelligence and robotics. Overall, only 21.94% of global patent applications for advanced technologies are owned by the EU27, a rather low figure. But the gap is perhaps even more striking when the EU's performance is compared with that of the U.S., China and Japan. Figure 2 shows the performance of these four entities in the segments examined highlighting the EU's vulnerabilities.

Given that we cannot consider digital sovereignty without a strong technological component, the EU's priority development area is to close the technological gap as soon as possible. However, there are several pitfalls. Firstly, there is the question of

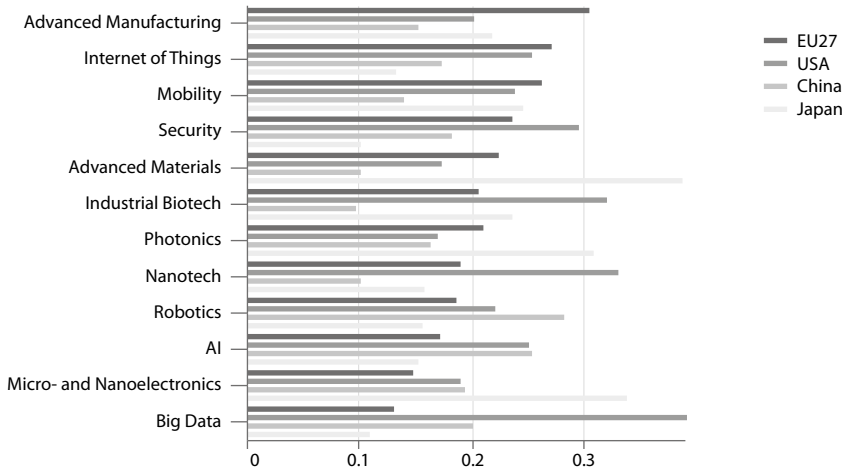


Figure 2. *The European Union's performance compared to other countries*

Source: European Parliament 2021: 20

the extent to which Member States are united in their perception of the importance of this area and their willingness to develop these sensitive areas. On the other hand, the availability of resources may be an issue. And this does not primarily refer to material resources (although these are finite), but to the raw materials needed for production. In this context, the availability of semiconductors is critical, as they are the building blocks of all digital products and thus the main drivers of the accelerating digitalisation industry.

In the last thirty years, the European Union has seen a very sharp decline in this area: while in 1990 the European semiconductor market share stood at 44% worldwide (Automotive News Europe 2021), it has now fallen dramatically to between 8–13% (Semiconductor Industry Association 2020), while the Asian region has a very high share of over 60% (see Figure 3). As a result, the market is dominated by a few leading chipmakers: in 2020, only two companies, TSMC (Taiwan) and Samsung (South Korea), were producing 5nm chips, and in Europe there are no companies producing sub-22nm components (European Commission 2021c). The U.S. company Intel has also postponed the introduction of 7nm components until 2022, which shows the technological complexity of chip manufacturing (European Commission 2021c: 82). At the same time, Intel could be the company that could save Europe: in 2021, it announced that it will set up a state-of-the-art semiconductor manufacturing plant in Europe by 2026, allowing EU companies to produce their own chips in Europe based on their own semiconductor designs (BERTUZZI 2021).

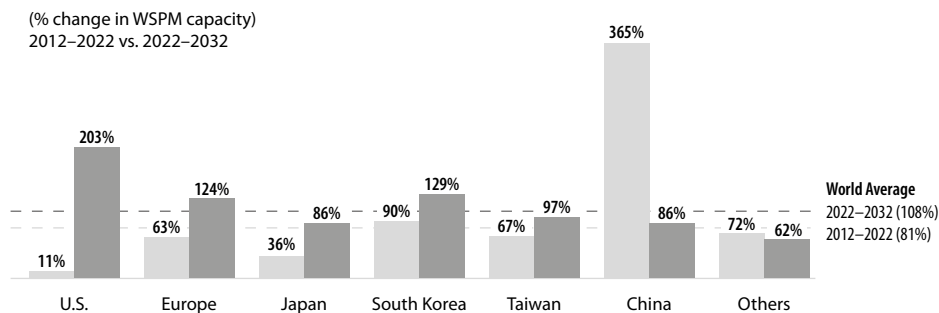


Figure 3. *Changes in global semiconductor capacity*

Source: Semiconductor Industry Association 2024: 10

If this is realised, European supply chains will be strengthened in the medium term. And Intel is on track, with plans to introduce 2 and 1.8nm technology for Intel 20A and 18A by 2024 (CONWAY 2024).

The specific case of Taiwan is particularly relevant for digital independence. This is because roughly two-thirds of the world's chips are currently produced on the island. Among other things, this is why developments in Taiwan in the summer of 2020 (and the more tense period of today) have been a cause for concern, as, if China were to intervene in Taiwanese trade, either by blockade or direct military strike, this would certainly have a longer-term impact on the U.S., Europe and the world's digital economy as a whole, given that the production and supply of basic infrastructure elements of cyberspace, such as computers, mobile devices and networking solutions, will be at stake, not to mention the automotive industry, which is of major importance to European industry. The most urgent step for digital autonomy is therefore to (re)build the semiconductor industry in Europe (HASS-BLANCHETTE 2022).

Finally, it is important to stress that this sector is very intensive in R&D, with up to a third of revenues being returned to research and therefore requires significant capital investment. It is not surprising that China is also at the forefront in this area. It aims to achieve 70% self-sufficiency in chip manufacturing by 2025 and has earmarked \$150 billion over 10 years for this purpose under the "Made in China 2025" program. South Korea plans to invest \$17 billion in next-generation chips by 2029, while the U.S. has a \$25 billion plan for R&D and manufacturing investment over 5 years (European Commission 2021c: 83). And where does the European Union stand in the queue? It seems to be catching up. The entry into force of the European Chips Act on 21 September 2023, which is expected to address the semiconductor shortage and strengthen the EU's technological sovereignty, thereby reinforcing

Europe's technological leadership, is a welcome development. It is expected to mobilise more than €43 billion of public and private investment by 2030 and, together with Member States and international partners, prepare to anticipate future supply chain disruptions and respond rapidly when needed (European Commission 2023).

CLOSING THOUGHTS

Currently, therefore, the U.S. and China are the two actors that can have a meaningful impact on shaping digital autonomy in Europe. The European Union is also actively trying to shape the rules of cyberspace, but the perceived East–West divide significantly reduces the chances of success in achieving its own strategic goals. At the same time, increasing geopolitical tensions are only one of the challenges to digital strategic autonomy. Future threats also include the widespread adoption of the Internet of Things (IoT),⁹ 5G, artificial intelligence, cloud and data-driven business models in both the economy and society, disruptive changes associated with the shift of (sovereign) power towards oligopolistic, trillion-dollar platforms; and the accompanying explosion of cybercrime and cyber threats. And finally, one cannot ignore the radically new technologies already mentioned, such as artificial intelligence, 5G/6G, advanced semiconductors and quantum technologies, most of which are emerging more or less simultaneously, and all of which are fundamental to the future of the EU (TIMMERS 2022: 39–40). In this perspective, it is no coincidence that in 2021 the European Union Agency for Cybersecurity (ENISA) has identified the following seven areas as key areas for the development of the EU's digital strategic autonomy: data security, trusted software platforms, appropriate incident management, trusted hardware platforms, post-quantum cryptography, user-friendly security tools and practices, and digital communications security. At the same time, ENISA added that, while digital autonomy and sovereignty relies on technological leadership – and most importantly on significant R&D – technical leadership alone is not sufficient to ensure sustainable strategic autonomy in the long run. The EU therefore needs the social science dimensions of digital autonomy, as well as a skilled workforce and the right legal and regulatory environment (ENISA 2021).

The time has come for the European Union to take the necessary steps to maintain its strategic autonomy in digital terms. It is important to note, however, that although the European Union is currently primarily a normative power, it has the potential to

⁹ Internet of Things describes a network of “things” (different collected devices and technology) embedded with software, sensors and other technologies to connect and exchange data with other devices and systems while using the internet.

maintain its strategic digital sovereignty as a geopolitical actor. However, if European industry does not shift up a gear and build its own capabilities in these years, it will find itself dependent on the U.S. and China for decades to come. And the loss of digital sovereignty means that Europe will fall out of the 21st century's centres of power and become a sphere of influence for an indefinite period. And while this is not a hopeless situation (think of China and its development over the last twenty years), it is one that can be avoided if the regulatory environment is well designed, and the necessary capacities are in place in time. Today, there is every chance that this will happen.

REFERENCES

- Automotive News Europe (2021): Europe Looks to Secure Chip Supply after 'Naive' Past Approach. *Bloomberg*, 5 May 2021. Online: <https://europe.autonews.com/suppliers/europe-looks-secure-chip-supply-after-naive-past-approach>
- BERTUZZI, Luca (2021): Leading Chip-maker Answers EU Call to Scale up European Capacity. *Euractiv*, 10 June 2021. Online: <https://www.euractiv.com/section/digital/news/leading-chip-maker-answers-eu-call-to-scale-up-european-capacity>
- BROWN, Ronald Harmon (1993): *The National Information Infrastructure: Agenda for Action*. Executive Office of the President, Information Infrastructure Task Force, September 1993. Online: <https://search.worldcat.org/title/30587669>
- CONWAY, Adam (2024): Intel's Process Roadmap to 2025: Intel 7, 4, 3, 20A, and 18A Explained. *QXDA*, 4 February 2024. Online: <https://www.xda-developers.com/intel-roadmap-2025-explainer>
- Council of the European Union (2003): *European Security Strategy. A Secure Europe in a Better World*. Online: <https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf>
- Council of the European Union (2022): *A Strategic Compass for Security and Defence. For a European Union that Protects Its Citizens, Values and Interests and Contributes to International Peace and Security*. Online: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>
- ENISA (2021): *Cybersecurity Research Directions for the EU's Digital Strategic Autonomy*. Online: <https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy>
- European Commission (1995): *Europe and the Global Information Society. Recommendations to the European Council. Conference G7 – Report Bangemann*. Luxembourg: Publications Office of the European Union. Online: <https://op.europa.eu/en/publication-detail/-/publication/44dad16a-937d-4cb3-be07-0022197d9453>
- European Commission (2009): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, COM(2009) 149 final, *Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience*. Online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52009DC0149>

- European Commission (2010): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2010) 245 final, *A Digital Agenda for Europe*. Online: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:en:PDF>
- European Commission (2013a): *Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure*. Online: <https://data.consilium.europa.eu/doc/document/ST-13280-2013-INIT/en/pdf>
- European Commission (2013b): Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013), 1 final, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Online: <https://www.eucybernet.eu/wp-content/uploads/2020/08/2013-cybersecurity-strategy-of-the-european-union.pdf>
- European Commission (2020a): Joint Communication to the European Parliament and the Council, JOIN(2020) 18 final, *The EU's Cybersecurity Strategy for the Digital Decade*. Online: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018>
- European Commission (2020b): *Commission Staff Working Document. Identifying Europe's Recovery Needs*. Online: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0098\(01\)&rid=3](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0098(01)&rid=3)
- European Commission (2020c): *Shaping the Digital Transformation in Europe*. Online: <https://digital-strategy.ec.europa.eu/en/library/shaping-digital-transformation-europe>
- European Commission (2021a): Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme "Path to the Digital Decade", COM(2021) 574 final. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0574>
- European Commission (2021b): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2021) 118 final, *2030 Digital Compass: The European Way for the Digital Decade*. Online: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118>
- European Commission (2021c): *Europe's Digital Decade: Digital Targets for 2030*. Online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
- European Commission (2021d): *Advanced Technologies for Industry*. Online: <https://ati.ec.europa.eu/>
- European Commission (2023): *European Chips Act*. Online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en
- European External Action Service (2016): *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*. Online: https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf
- European Investment Bank (2016): *Restoring EU Competitiveness. 2016 updated version*. January 2016. Online: https://www.eib.org/attachments/efs/restoring_eu_competitiveness_en.pdf
- European Organisation for Security (2019): *EU Digital Autonomy: Challenges and Recommendations for the Future of European Digital Transformation. EOS Position Paper*, November 2019. Online: <https://www.eos-eu.com/Files/EOSEUDigitalAutonomyPositionPaper.pdf>
- European Parliament (2011): *Critical Information Infrastructure Protection: Towards Global Cyber-Security*. Resolution 2011/2284. Online: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1479216690655&uri=CELEX:52012IP0237>

- European Parliament (2018): Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on *A Framework for the Free Flow of Non-Personal Data in the European Union*. Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1807>
- European Parliament (2019): Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on *Open Data and the Re-Use of Public Sector Information*. Online: <https://eur-lex.europa.eu/eli/dir/2019/1024/oj/eng>
- European Parliament (2021): *Europe's Digital Decade and Autonomy*. Online: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU\(2021\)695465_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695465/IPOL_STU(2021)695465_EN.pdf)
- European Parliament (2022): Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on *European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act)*. Online: <https://eur-lex.europa.eu/eli/reg/2022/868/oj>
- European Parliament (2024): Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (*Artificial Intelligence Act*). Online: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- GODEMENT, François – STANZEL, Angela – PRZYCHODNIAK, Marcin – DRINHAUSEN, Katja – KNIGHT, Adam – KANIA, Elsa B. (2018): *The China Dream Goes Digital: Technology in the Age of Xi*. *European Council on Foreign Relations*, 25 October 2018. Online: https://ecfr.eu/publication/the_china_dream_digital_technology_in_the_age_of_xi
- HASS, Ryan – BLANCHETTE, Jude (2022): *Central Questions in U.S.–China Relations amid Global Turbulence*. *Center for Strategic and International Studies*, 21 July 2022. Online: <https://www.csis.org/analysis/central-questions-us-china-relations-amid-global-turbulence>
- KASPER, Agnes – OSULA, Anna-Maria – MOLNÁR, Anna (2021): *EU Cybersecurity and Cyber Diplomacy*. *IDP Journal of Internet Law and Politics*, (34), 1–15. Online: <https://doi.org/10.7238/idp.voi34.387469>
- MOLNÁR, Anna (2016): *Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája* [Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy]. *Nemzet és Biztonság*, 9(2), 75–85.
- MOLNÁR, Anna (2022): *European Union – Cybersecurity*. In MOLNÁR, Anna – MÁRTONFFY, Balázs (eds.): *Cyber Diplomacy from the European Perspective*. Budapest: Ludovika University Press, 43–71. Online: https://doi.org/10.36250/01039_02
- MOLNÁR, Dóra (2022): *Great Power Cyber Diplomacy: China on the International Cyber Platform Accompanied by the United States and Russia*. *Hadtudomány*, 32(E-szám), 227–241. Online: <https://doi.org/10.17047/Hadtud.2022.32.E.227>
- POGOREL, Gerard – NESTORAS, Antonios – CAPPELLETTI, Francesco eds. (2022): *Decoding EU Digital Strategic Autonomy. Sectors, Issues, and Partners*. Brussels: European Liberal Forum. Online: https://liberalforum.eu/wp-content/uploads/2022/06/Decoding-EU-Digital-Strategic-Autonomy_ELF-Study_Techno-Politics_vol.1-2.pdf
- Semiconductor Industry Association (2024): *State of the U.S. Semiconductor Industry*. Online: https://www.semiconductors.org/wp-content/uploads/2024/10/SIA_2024_State-of-Industry-Report.pdf

- STOLWIJK, Claire (2022): Strengthening Digital Sovereignty Makes Europe Less Vulnerable both Politically and Economically. *TNO*, 14 June 2022. Online: <https://www.tno.nl/en/newsroom/insights/2022/06/strengthening-digital-sovereignty-makes>
- THIEULIN, Benoît (2019): *Towards a European Digital Sovereignty Policy*. ESEC's opinion, March 2019. Online: https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf
- TIMMERS, Paul (2022): Cybersecurity and Resilience from a Strategic Autonomy Perspective. In POGOREL, Gerard – NESTORAS, Antonios – CAPPELLETTI, Francesco (eds.): *Decoding EU Digital Strategic Autonomy. Sectors, Issues, and Partners*. Brussels: European Liberal Forum. Online: https://liberalforum.eu/wp-content/uploads/2022/06/Decoding-EU-Digital-Strategic-Autonomy_ELF-Study_Techno-Politics_vol.1-2.pdf
- VECSEY, Mariann (2019): Changes in the Migration Trends from West Africa to Europe. *Hungarian Defence Review*, Special Issue, 147(1–2), 99–116. Online: <https://doi.org/10.35926/HDR.2019.1–2.8>
- ZHANG, Yingying – ZHOU, Yu (2015): *The Source of Innovation in China*. London: Palgrave Macmillan. Online: <https://doi.org/10.1057/9781137335067>