CIDOB briefings

ISSN 2564-8713

42
DECEMBER
2022

# HOW CAN THE EUROPEAN UNION ACHIEVE DIGITAL STRATEGIC AUTONOMY? Views from future leaders

**Inés Arco Escriche,** Researcher, CIDOB

*This document is based on the debates of the Santander-CIDOB Future Leaders Forum online session titled "How can the European Union achieve digital strategic autonomy?" that took place on November 8th, 2022; and the video interviews with the selected young leaders from the 35 under 35 List. The document is structured in two blocs: first, it introduces the current debates and challenges for the EU's advancement on its digital sovereignty and strategic autonomy; and second, it highlights five areas of essential relevance for its digital ambitions identified by the participants. The text was finalized on December 23rd, 2022.*

We live in a technopolar moment. In the current context defined by a fragmented digital landscape, technology and digitalization act as (re)distributors of power in the international system – and within societies –, and as catalysts of global powers and large technology firms' geopolitical and economic ambitions. The weaponization of digital tools and technology has become a core aspect of the current strategic competition, leading to increasing feuds around critical digital infrastructures, key industries such as AI or semiconductors, essential elements for production, like rare earths; and the control of data. Thus, states increasingly view access to new and critical technologies as a necessity to secure their sovereignty, both in the physical and digital space. Advances in new technologies – and those who control them – will undoubtedly shape the future global order.

In this ongoing technological revolution, the necessity of the European Union (EU) to advance toward strategic autonomy and achieve digital sovereignty have become two priorities of the von der Leyen Commission. The EU aims to develop and control new technologies within its own borders, reasserting its sovereignty in the digital domain. Yet, Brussels may need to balance the regulation of the unruly digital sphere following a model in line with democratic tradition and liberal values with the provision of public digital and cyber goods while addressing its current weaknesses in the digital and technological domain.

## 1. The EU's quest for a digital strategic autonomy: an evolving definition

Strategic autonomy is often defined as the ability of the EU to mobilize the necessary means to achieve its foreign policy aims in cooperation with partners, when possible, but acting alone when necessary (Morillas, 2021).

Nevertheless, since 2016, the scope and definition of strategic autonomy have evolved as reactive reasoning to the changing geopolitical environment and the EU's interests and needs. The concept, born as a notion related to security and defence policies, has morphed into a wider buzzword to include most of Europe's weaknesses, dependencies, and imbalances in multiple areas, such as trade relations. First, due to the antagonistic geopolitical environment marked by Brexit, uncertainty under the Trump Administration and China's assertiveness in the middle of the trade war. Second, the pandemic of COVID-19 and the war in Ukraine led to a newfound awareness of economic interdependence and the increasing trends of hybrid and cyber threats. Thus, the current concept of strategic autonomy goes beyond defensive integration and has opened the scope to virtually all kinds of EU policy areas, encompassing energy, rare earths, and technology among others.

The focus on technological and digital sovereignty – key components of the strategic autonomy of the EU as digitalization becomes critical for geopolitical power and economic interests – has increased during the von der Leyen Commission. The relevance of this area came after the emerging importance of the data economy, growing concerns about the influence and power consolidation in a few non-EU technology companies; and the potential dependence on foreign technologies, critical infrastructure, digital services and data control and protection from foreign actors (EPRS, 2020). According to the European Political Strategy Centre (2019), 'digital sovereignty' refers to Europe's ability to act independently in the digital world, through protective mechanisms, offensive tools and cooperation with key actors while fostering digital innovation. Besides, the concept is linked to the promotion of its own values and the safeguarding of its interests in a wide spectrum of strategic areas such as cybersecurity, data protection, cloud storage or the development of ethical AI.

Yet, the narrative and the lack of a clear, official definition have been quite ambiguous on the meaning of what is a technological and digital strategic autonomy – especially when terms such as "technological sovereignty", "digital sovereignty" or "digital strategic autonomy" are used interchangeably. In other words, this vague approach to digital strategic autonomy should be first better conceptualized, finding consensus on the interests, principles, and benefits of such endeavour. Consequently, two elements need to be highlighted.

> A digital strategic autonomy based on isolation and autarky is technologically impossible and politically inconvenient in the existing landscape.

First, increasing connectivity and dependencies on digital services and key components for the development of digital technologies considered as a vulnerability have given rise to positions easily mistaken for protectionism. However, the EU's bid for digital strategic autonomy must not be equated to the EU being isolated from other actors. Elements such as semiconductors – the backbone of digital technologies – are part of a very complex manufacturing process and industry, which includes a high division of labour, huge capital, very specialized knowledge, and long manufacturing times. No region or actor in the world can procure all necessary inputs locally nor can it perform all manufacturing steps. Thus, transnational dependencies will continue no matter how much financial capital and subsidies are devoted towards this end (Kleinhans and Hess, 2022). Additionally, in the transition from a fossil fuel society towards a green economy, new dependencies will arise in the development of these green technologies needed – such as solar panels. Therefore, a digital strategic autonomy based on isolation and autarky is technologically impossible and politically inconvenient in the existing landscape.

Secondly, even if international cooperation, multilateralism and coordination with allies and partners are at the core of the effort, it does not mean that the EU should leave unquestioned important relations with allies and partners. As we have seen, the concept itself evolved in times when the transatlantic relation was weakened under the Trump administration. The EU must rethink and revalue the impacts that internal and international changes could have on its key interests and security, as it advances and progresses towards digital sovereignty. Here, the key is its empowerment in the digital and technological domain.

Thirdly, in the current context marked by an acceleration of existing systemic competition between the US and China and the trend towards *sectorial decoupling* and *fragmented regulation*, the EU should have its own purpose. In the area of technology, there are completely different and overlapping visions of its use, standards and the rules of the Internet for China and the US. This increasing confrontation, which goes beyond technology, has led to a simplistic narrative of a world of two blocs or a new Cold War competition. However, as the present is defined by complexity, hyperconnectivity and deep economic and digital interdependences, the EU should avoid failing trap of this narrative – accepting it, would indicate that the EU is being dependent on one of the sides. To break and get rid of these dependencies means building a European model to approach technology, establishing itself as an alternative in the current technological development competition divided between the Silicon Valley model and the technoauthoritarian model.

## 2. The three challenges to the EU's response to technology and digital sovereignty

The EU's position as a trade and normative power has encouraged an approach focused on consumers – opposed to the geopolitical, security and military logic that has underpinned the technological transformation in the US, Russia and China. The EU's technology capacity is closer to the reality of India or Japan, with important disparities between member states in digital and cyber capabilities and technological industries. This nature of the EU has prompted a responsive approach to technology, usually as a late response to a trend that has been going on for more than two decades. Technology and information have been long conceived as tools of power for other actors – transmitting their ideology in technological development and research.

The goals of the EU's push for greater digital sovereignty are three-fold. First, the development of EU-based technological capabilities through innovation and industrial competitiveness. Second, the establishment of global gold standards in digital regulation and standards in line with the EU values, especially for the digital economy. Finally, the assertion of its sovereignty in the digital domain by reducing exposure to external actors, such as tech companies or governments (Burwell and Propp, 2022).

In the new geopolitical Europe of the von der Leyen Commission, these objectives have promoted new responses from the EU as a result of economic necessity and political vertigo. Brussels has advanced multiple normative and regulatory frameworks in the areas of data protection, ethical and human-centric approaches to technology, online platforms' responsibilities or tackling disinformation. However, regulation alone cannot guarantee European technological independence and thus, the EU has also directed efforts to reduce dependencies and ensure a "security of supply", as well as increasing research, capability development and directing investment in key strategic areas for innovation, digitalization and security.

To guarantee the EU's technological and digital sovereignty, efforts need to be coordinated and comprehensive, with substantial resources directed towards increasing internal resilience, innovation and the development of key infrastructures and emerging disruptive technologies.

To guarantee the EU's technological and digital sovereignty, these efforts need to be coordinated and comprehensive, with substantial resources directed towards increasing internal resilience, innovation and the development of key infrastructures and emerging disruptive technologies – including quantum computing, cloud services, AI or blockchain technologies among many. Here, multiple challenges arise:

The first challenge is the existing difference in internal disparities between the EU member states and the lack of a real political union. On the one hand, member states present a plurality of positions regarding strategic autonomy and digital sovereignty – with differing degrees of support and opposition regarding constraints in trade, industry, and the possibility of overlapping commitments between the EU's defence policy and NATO. On the other, their internal capabilities in technology and digital domains are unequal, with varying interests and dependencies, which may hinder a consensus between the 27 EU Member states and the subsequent adoption of a common regulatory framework that systematizes their position in various key technological areas. For example, nine member states have published their own positions on how international law applies to cyberspace while failing to promote a common agreement for a shared EU position on this matter. Addressing internal digital divides and asymmetric frameworks will be key to building the EU's role – even with its weaknesses.

Secondly, while the EU is advocating for an "open strategic autonomy" - based on openness and competitiveness in global trade and investment -, digital strategic autonomy may imply the re-examination of free trade, open markets and related vulnerabilities that exist in these domains. For some, protecting Europe's sovereignty – advancing geopolitical logic rather than purely market or economic interests – may require the adoption of defensive measures, such as limiting non-EU actors' access to the EU Single Market or the control and securing of data flows and key strategic technologies, as in the case of 5G providers. However, these measures may also go against certain rules of free trade in the current global economic order. Thus, the fragile balance to continue harvesting the benefits of a rule-based free market while also protecting the EU's interests shows a significant challenge to the discourse and practice of real strategic autonomy.

Thirdly, the debate should address the difficulties of a global governance framework for the Internet and the technologies of tomorrow. The fragmentation of cyberspace and the Internet – especially by authoritarian regimes – should encourage the debate on the creation of references and limits to the extraterritoriality and deregulation of big technological actors. It's in this context the Brussels effect can blossom and the GDPR and Digital Services Act (DSA) model may be able to make a difference. The first hint is the changing role and responsibilities of tech platforms in fighting disinformation, which has been later replicated in agreements with tech giants in many countries, especially in Latin America. The current reputational crisis – exemplified by the debate around the limits of monopolistic power in these entities – may have an impact on the transformation of the sector and the role of tech platforms. In this vacuum, the EU has an opportunity to set the rules – which is what's currently happening. The question is if the European success as a regulatory power with the development of the Single Market and the GDPR – recreated around the world – may be able to emulate the same process in the field of technology. To create global standards, the EU must also be able to deliver significant public technological and cyber goods and deploy strong digital diplomacy to attract countries to join, first strengthening existing capabilities within the EU. In conclusion, the EU must be able to integrate internal and external dimensions of its policies, balancing internal market concerns, fundamental rights and geopolitical concerns to successfully advance its digital strategic autonomy.

In conclusion, the EU must be able to integrate internal and external dimensions of its policies, balancing internal market concerns, fundamental rights and geopolitical concerns to successfully advance its digital strategic autonomy.

## 3. A multidimensional approach to Europe's digital strategic autonomy

Considering the current challenges and developments, the EU can advance its digital strategic autonomy by making progress in five different areas:

**Redefining strategic thinking on digital strategic autonomy and security**

As EU Commissioner for Internal Market, Thierry Breton, mentioned the EU lacks a doctrine in cyberspace. The current approach has relied on deterrence, focusing on denial and punishment – for example, through sanctions – with limited results in hampering malicious cyber activities. As stated in a report published by European Union Agency for Cybersecurity in November 2022, cybersecurity attacks have increased during the second half of 2021 and 2022, with a fivefold increase of attacks on cloud infrastructure in a year – narrowly linked with the impact of Russia's invasion of Ukraine in cyber warfare.

The EU approach to cyber threats should avoid the adoption of defensive and bold actions since it may encourage other actors to do the same, including competitors and rivals, and fuel a cyber arms race. Therefore, the EU should systematically secure the underlining structure within its borders and with partners to reduce the impact and scale of attacks. Achieving this defence superiority policy can be done by encouraging open-source security, encryption in critical systems and rolling out multifactor authentication on a massive scale while making it easier to transform cyberspace into a safer environment (Weber, 2022).

Cybersecurity has a crucial role in this aspect. Cybersecurity products, standards, practices and responses need to be understood as a nexus within the EU's strategic autonomy, which also implies strong international cooperation. The current policy initiatives in this field are focused on cybersecurity capacity building and collaboration among member states. Yet, there are still significant cybersecurity skills gaps – as the increasing demand for such services has not been yet met in terms of labour.

**Unleashing the potential of participatory democracy and diversity to create efficient digital policies**

While most people trust the technology sector, a third of Europeans are concerned about data privacy. The rapid, unregulated technological revolution, growing disinformation and the development of disruptive technologies – which impact privacy and data protection – are eroding societies' trust in these advances, increasing concerns over surveillance by states or companies.

Therefore, any European effort towards digital strategic autonomy must consider citizens and the impact of these decisions on their lives. Awareness raising, capacity building and skills acquisition will be key for EU citizens to be part of the transformation as well as to identify new solutions and responses. In 2021, only 54% of people in the EU between 16 to 74 years old have basic overall digital skills. Access to hardware and software and the development of significant skills to use the cyberspace and the Internet in a way that empowers citizens and those traditionally left by current transitions – such as low-income populations or people living in rural areas – should be a priority. Active participation in the digital domain can help distribute knowledge around society and encourage creativity and innovation to foster the EU's internal capacity and talent acquisition.

Additionally, these new digital technologies also offer opportunities to improve law and policymaking in the digital field. These tools can allow the involvement of Europeans in the decision-making process harvesting the benefits of digital participatory democracy to create meaningful and effective policies around digitalization and the EU's digital strategic autonomy. Tools such as passive citizens' sourcing, online deliberation and online citizen engagement and participation can be included and mainstreamed through the policy cycle, including issue identification, agenda setting, policy adoption or evaluation. Centring people in the EU's strategic thinking on digital can lead to global leadership by prioritizing digital rights and access, together with meaningful

To create global standards, the EU must also be able to deliver significant public technological and cyber goods and deploy strong digital diplomacy to attract countries to join this model.

inclusion in decision-making – while also advancing transversal challenges such as gender equality.

### Developing a comprehensive alternative model through regulation

While the EU initially stayed on the sidelines of the technological competition, it is currently playing a key role in regulation, standard settings, and the development of norms in cyberspace. The success of previous examples shows how regulation goes beyond being a technicality, to become an important geopolitical opportunity to ensure that norms are created with European values, human rights, and a people-centric approach at the core. These regulations efforts in areas such as fighting disinformation, introducing limitations for big tech companies, creating a Single Data Space in the EU based on convergence; new technical standards for disruptive technologies; and the publication of a common position on the application of international law in the cyberspace can help the EU to strengthen its role as an international player.

Centring people in the EU's strategic thinking on digital can lead to global leadership by prioritizing digital rights and access, together with meaningful inclusion in decision-making.

However, as technology progresses, laws become outdated and new regulatory efforts seem to be conducted in a reactive response rather than based on anticipation and the regulation of the technologies of tomorrow. Calls for fighting disinformation and establishing limits for big technological actors come after the stark evidence of the negative impacts of social media on society, and the lack of accountability and responsibility from these actors. While creating a shared framework for regulating tech companies is an important political battle for the EU and is indeed needed, its ambitions should anticipate other future challenges. Capitalising on this ability to set the tone, the EU should also focus on regulating the technologies of tomorrow, such as 6G or the Internet of Things where no actor is leading yet.

Additionally, the EU should learn from previous weaknesses. The enforcement and actual implementation of the GDPR is far from ideal – and it's at risk if additional resources and efforts are not put into personal data policy. The lack of substantial resources directed towards these regulations and failing to articulate a comprehensive and coordinated effort towards these policies – while settling for a patchwork approach too stringent for the nascent data economy – may reduce their impact. Thus, regulation must be backed up with resources, strong coordination and monitoring activity and solid diplomatic efforts coupled with indigenous technological input that attract and invite others to join this model.

### Industrial policy, research, investment and strengthening supply chains

As the geopolitical context may evolve into an international system defined by power, with increasing relocalisation and decoupling dynamics, the EU must be prepared to respond to emerging challenges in this area. However, while the EU may be starting in a position of weakness in front of other competitors, partly due to its lack of digital giants or strategic dependencies on rare earths, semiconductors or cloud computing; it still has some assets and significant room to manoeuver to be a relevant player in the technology battle.

First, the EU should consider the development of a technological-focused industrial policy to reduce internal gaps in technological capabilities and know-how, coupled with solid investment commitments to enhance the development of alternatives for key digital services, such as cloud or new computing resources in key areas like quantum and edge technologies. Besides developing key infrastructures, creating building-value digital solutions in specific domains where the EU has a significant advantage – such as healthcare or anti-money laundering – also have the potential to position Europe at the forefront of these sectors. Here, investing in research and building public-private partnerships to attract, support and retain European and international talent to foster innovation will be crucial.

To do so, the EU should direct persistent and substantial investments to ensure innovation and the development of indigenous disruptive technologies with a long-term horizon. It would be also important to identify in which areas the EU can acquire an effective advantage while focusing on diversification in strategic dependencies in products with complex ecosystems and securing supply chains through strong coalitions with allies and partners, where self-sufficiency isn't realistic. In conclusion, the EU needs to develop adding-value solutions through investments, action plans that foster synergies in the cyberspace and defence industries while addressing internal digital divides and asymmetric frameworks to build a comprehensive role for the EU.

### Building alliances and fostering international cooperation

International cooperation beyond the EU is fundamental for achieving digital strategic autonomy and ensuring coordination in multiple domains – such as regulation and standard settings, but also supply chain security or secured data flows. To achieve this objective, the EU must have a clear dedication to multistakeholder partnerships and alliances, including academia, civil society, NGOs, industry, and tech companies as well as other governments and international organisations, putting trust at the centre of any effort. Coordination, engagement, and dedication to multilateralism to advance the EU's interests in the digital sphere are a necessity – especially in the UN, where the next three years of discussions will be decisive.

International dependencies are the fundament of many production and operating processes in key digital technologies, such as in the semiconductor industry, data and cloud storage or critical infrastructures. A mapping and assessment of their security and resilience should be conducted systematically. Addressing key elements that threaten the functioning of these technologies, with dramatic effects in multiple industries, requires addressing bottlenecks and vulnerabilities. Facing these challenges can only work in cooperative and organized responses through international partnerships with trusted countries around the world.

Finally, while strengthening the domestic industrial technology sector can increase the sense of security of the EU, its quest for strategic autonomy should also include helping others to achieve their own digital strategic autonomy. Today's choices in countries around the world on technologies and infrastructure will create path dependencies for the future and ensuring cooperation in technology can contribute to guaranteeing a digital transition that reflects European values globally. Facilitating international knowledge exchange for innovation, also including best practices and response mechanisms to respond to borderless threats can also contribute to the EU's leadership in this area. Only through solid digital diplomacy and efforts towards cooperation can the EU become digitally autonomous.

## References

Burwell, Frances; and Propp, Kenneth. «Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy». Washington, D.C: Atlantic Council Europe Center, 2022. (online) https://www.atlanticcouncil.org/wp-content/uploads/2022/11/Digital-sovereignty-in-practice-The-EUs-push-to-shape-the-new-global-economy_.pdf

European Parliamentary Research Service. *Digital Sovereignty for Europe*. EPRS Ideas Paper, 2020. (online) https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

European Political Strategy Centre. *Rethinking Strategic Autonomy in the Digital Age*. EPSC Strategic Notes 30, 2019. (online) https://www.almendron.com/tribuna/wp-content/uploads/2019/11/rethinking-strategic-autonomy-in-the-digital-age.pdf

Kleinhans, Jan-Peter, and Hess, Julia. *Analysis of the EU Chips Act: The Crisis Response Toolbox*. Berlin: Stiftung Neue Verantwortung, 2022. (online) https://www.stiftung-nv.de/sites/default/files/governments_role_in_the_global_semiconductor_value_chain_3_0.pdf

Morillas, Pol. «Afghanistan, AUKUS and European Strategic Autonomy». JOINT Policy Brief nº4, 2021. (online) https://www.cidob.org/es/publicaciones/serie_de_publicacion/project_papers/joint/afghanistan_aukus_and_european_strategic_autonomy

Weber, Valentin. *Rethinking European Cyber Defense Policy.* DGAP policy Brief No.8, 2022.(online) https://dgap.org/en/research/publications/rethinking-european-cyber-defense-policy