
European Union flag formed by binary code. Image: Shutterstock.

Defending EU Democracy and Sovereignty from the New Geopolitics of Technology

José Ignacio Torreblanca

CEBRI JOURNAL

Year 4 / No. 16 / Oct-Dec 2025

SPECIAL SECTION

Defending EU Democracy and Sovereignty from the New Geopolitics of Technology

José Ignacio Torreblanca

Abstract: This article argues that technology is a central dimension of international power, reshaping geopolitics through data, standards, platforms, and supply chains, while US–China rivalry drives securitization, selective decoupling, and technological spheres of influence, and private firms provide critical security infrastructures. As the US leverages the EU's technological dependencies to pressure regulatory change and influence its domestic politics, the European Union faces an existential challenge. Regulatory leadership alone, the article concludes, is insufficient; capabilities to reduce dependencies, safeguard democracy, and strengthen technological sovereignty are also required.

Keywords: technological sovereignty; geopolitics of technology; artificial intelligence; democracy; European Union.

Defendendo a democracia e a soberania na União Europeia diante da nova geopolítica da tecnologia

Resumo: Este artigo argumenta que a tecnologia é uma dimensão central do poder internacional, reconfigurando a geopolítica por meio de dados, padrões, plataformas e cadeias de suprimento, enquanto a rivalidade entre Estados Unidos e China impulsiona a securitização, o desacoplamento seletivo e esferas de influência tecnológica, e empresas privadas fornecem infraestruturas críticas de segurança. À medida que os Estados Unidos exploram as dependências tecnológicas da União Europeia para pressionar mudanças regulatórias e influenciar sua política interna, a União Europeia enfrenta um desafio existencial. A liderança regulatória, conclui o artigo, é insuficiente; são também necessárias capacidades para reduzir dependências, salvaguardar a democracia e fortalecer a soberania tecnológica.

Palavras-chaves: soberania tecnológica; geopolítica da tecnologia; inteligência artificial; democracia; União Europeia.

THE RETURN OF HISTORY

Today, the great powers–fully aware that access to, control of, and mastery of critical technologies are indispensable requirements for their strategic survival–have entered an increasingly intense competition to secure their digital and technological sovereignty. This rivalry is not limited to the economic realm; it spans military, political, cultural, and normative dimensions. Technology has thus become a structural factor of power and international rivalry, on a par with territory, population, or natural resources. As technological dependencies become increasingly weaponized to coerce States into aligning with major powers' foreign policy objectives or to shape their domestic policy choices, the European Union—like other middle powers that neither lead nor fully control these emerging technologies—faces growing challenges to the resilience of its democratic institutions and the integrity of its technological sovereignty.

This phenomenon is not new. Throughout history, major technological revolutions have acted as precursors to major systemic changes, triggering profound economic, social, and political transformations both within societies and in the configuration of the international system and relations among its units. These changes have often unleashed significant conflicts, both within and among States.

Around 7,000 years ago, the shift from subsistence to intensive agriculture reorganized society. Surpluses allowed labor specialization and the emergence of durable political institutions: bureaucracies, taxation, standing armies, and religious hierarchies. Law and knowledge were codified, long-distance trade expanded, and authority concentrated in strategic centers, producing complex State structures and "hydraulic empires" built on control of water and agricultural resources, as well as the capacity to finance and arm large armies.

The first industrial revolution (1760-1840), driven by the steam engine, textile mechanization, and coal, shifted economies from agrarian to industrial foundations while eroding *Ancien Régime* structures and accelerating liberal economic and political change. Urbanization created new classes–the industrial bourgeoisie and the proletariat–whose demands transformed political representation. The American and French revolutions challenged Europe's monarchical order and unleashed conflicts that culminated in the Congress of Vienna (1814) and a new balance of power.

José Ignacio Torreblanca *is a senior lecturer in Political Science at UNED University in Madrid and Distinguished Policy Fellow at the Geoconomics and Technology Program at the European Council on Foreign Relations (ECFR). He was a Fulbright scholar at George Washington University and a postdoctoral fellow at the European University Institute.*

The second industrial revolution (1860-1930), based on electricity, railways, telegraphy, and steamships, amplified States' power projection by reducing transport and communication costs and integrating markets. Western technological superiority enabled low-cost imperial expansion; nineteenth-century conquest, including in Africa, relied on steamships, machine guns, and quinine (Headrick 1979). Rivalries among empires helped set the stage for World War I and Europe's long decline.

In Asia, technological lag proved costly: Qing China's failure to adopt industrial technologies produced defeats and the "Century of Humiliation," shaping today's emphasis on technological security, while Japan's isolation ended abruptly in 1853 with Perry's "black ships."

The third industrial revolution (1970-2000), centered on Information and Communications Technology (ICT), digitization, automation, and financial liberalization, powered globalization of value chains and capital flows. As innovation diffused from the West, its exclusive predominance eroded and a more multipolar order emerged; China's rise revived debates about power transitions and the risk of conflict (Allison 2017).

Now, as the fourth industrial revolution, beginning around 2010 with advances in robotics, global connectivity, and artificial intelligence (AI), unfolds, these transformations are felt in an even more distinctive way. The center of gravity of corporate power has shifted from traditional sectors–such as energy or finance–toward the technology sector.

For Europe, the new geopolitics of technology implies moving from the dependencies and vulnerabilities associated with oil and gas from the Middle East and Russia to being trapped in a new dependence on artificial intelligence models, data centers, semiconductors, and other technologies contested between the United States and China.

This shift has prompted growing State intervention in spheres previously regarded as predominantly private. Great powers now compete to control the strategic chokepoints of the digital economy: data, algorithms, connectivity infrastructure, and computing capacity. In this context, artificial intelligence has become a central field of geopolitical rivalry, especially between the United States and China, with direct implications for alliances, international norms, and balances of power. AI is not only transforming productive and labor relations within States;

it is reconfiguring the architecture of global power by introducing new asymmetries and technological dependencies. As in previous technological revolutions, those who manage to master these capabilities will largely define the rules of the twenty-first century international order and the hierarchy of power within it.

The international consequences of this reconfiguration of the world around digital technologies are clear. Just as the economy based on the exploitation of fossil fuels generated an international order and a set of alliances linked to access to and control of production centers in the Middle East and the Persian Gulf, today's economy–based on the exploitation of data–is generating its own system of international relations, based on access to critical raw materials to feed that technological development and on supply chains and production and distribution centers and networks for digital technologies. For Europe, the new geopolitics of technology implies moving from the dependencies and vulnerabilities associated with oil and gas from the Middle East and Russia to being trapped in a new dependence on artificial intelligence models, data centers, semiconductors, and other technologies contested between the United States and China.

THE NEW GEOPOLITICS OF TECHNOLOGY

Three novel elements distinguish today's technological transformation from previous revolutions.

First, the speed, scope, and depth of current technological changes, especially regarding global connectivity and the diffusion of innovations. Whereas key twentieth-century technologies, such as the telephone, needed nearly half a century to reach one million users and a century to reach one hundred million, contemporary tools based on generative artificial intelligence, such as ChatGPT, reached one million users in five days and 100 million in five months (Hu 2023).

A second novel element concerns the transformation of the concept of security induced by technological development. Alongside the traditional domains of war–land, sea, air, and space–a fifth operational domain has emerged: cyberspace, which includes not only attacks on critical infrastructures–with growing potential due to increased connectivity of multiple devices, i.e., the Internet of Things–, but also the manipulation of the informational or cognitive space.

Authoritarian regimes, especially Russia and China, have found in the openness and lack of regulation of social media platforms in the West a very effective instrument to bolster their power, both inward and outward. As the director of Russia's State media, Margarita Simonyan, noted, Russia Today, Sputnik, and the

global network of Russian media exist for the same reason the Russian Ministry of Defence exists: "to wage an information war against the West" (Torreblanca 2020).

Disinformation phenomena demonstrate how manipulation of the information space can have strategic consequences comparable to those of traditional military instruments, and how certain actors can exploit these tools to their advantage.

A third distinctive element of today's technological revolution is the central role of private technology companies as providers of services essential to national sovereignty. Today, a substantial portion of the critical infrastructures that sustain the functioning of advanced economies is in the hands of private companies, without the State having the technical, financial, or time capacity to replace them. This is the case for cloud computing services, advanced semiconductor manufacturing, the deployment and maintenance of submarine communications cables, or low-orbit satellite networks. These infrastructures are crucial both for economic activity and for military and intelligence capabilities, yet they far exceed the public sector's capacities (Torreblanca 2023).

The conflict in Ukraine has highlighted this new reality. Western–particularly US–technology companies such as Microsoft, Amazon, Palantir or Starlink have played a key role in securing Ukraine's critical digital infrastructures, providing key services to its Armed Forces (especially regarding data acquisition and processing). The growing fusion between the US Pentagon and certain software and digital services companies specialized in the military domain, such as Anduril or Palantir, paints an extremely worrying scenario. Just as Eisenhower warned in 1953 about the power of what he called the "military-industrial complex," this concern about the structural power of private companies and their link to national sovereignty led President Biden to issue a similar warning in his farewell address about the "technological-industrial complex" and the consequences for democracy in the US and worldwide of the enormous concentration of power in the hands of a small number of technology companies (Biden 2025; Bria 2025).

Following President Trump's inauguration in January 2025, major US tech companies have succeeded in getting the White House to adopt as its own their long-standing grievances and demands against legislation on digital services and markets, giving way to a frontal attack and a series of open coercive measures against the EU, the United Kingdom and, among others, Brazil.

All these transformations have profound implications for international security. Traditionally, technological evolution and military doctrine tended to advance in relatively synchronized fashion, granting States and their armed forces sufficient time to adapt their organizational structures, strategies, and defense industries. In

the current context, however, the pace of technological innovation far exceeds the cycles of planning, acquisition, and deployment of military capabilities, whose time horizons are necessarily longer. As a result, technological acceleration introduces high levels of strategic uncertainty, making it harder to anticipate threats and formulate stable doctrines (Frías 2024).

Henry Kissinger drew attention to this problem in one of his last works (Kissinger et al. 2021). The international order after the Second World War was stabilized by the existence of nuclear weapons, which not only established a clear and widely recognized hierarchy of power, but also enabled the development of a rational, explicit, and shared theory of deterrence, regardless of ideological differences among actors. Possession of nuclear weapons–measurable and verifiable–facilitated strategic predictability.

In the case of artificial intelligence, however, Kissinger warned that the attempt to turn this technology into a vector of military power faces a fundamental challenge: the difficulty of building an effective theory of deterrence based on a technology whose limits, capabilities, and effects remain largely uncertain. Unlike the nuclear weapon, whose use in the Second World War allowed the consolidation of a theory and practice of deterrence and even the establishment of limitation and non-proliferation agreements, artificial intelligence could prove strategically more effective as a covert capability, susceptible to being used unilaterally and unexpectedly to launch preventive attacks. This feature increases uncertainty and raises the risk of systemic instability.

If artificial intelligence constitutes, as Kissinger suggested, the contemporary equivalent of a new Manhattan Project, the central challenge lies not only in its technological development, but in the creation of a deterrence and international governance framework capable of stabilizing its use and avoiding dynamics of uncontrolled escalation. Without a theory of deterrence adapted to this new technological reality, the risk is not the absence of balance, but the generation of an international order that is structurally more unstable.

SECURITIZATION AND DECOUPLING

The dominant geopolitical impulse today is characterized by growing securitization of technology. States no longer conceive technological innovation primarily as a factor of economic efficiency or social welfare, but as a strategic resource of power. Consequently, each technological advance is evaluated according to two central criteria: the relative power it can confer on third parties and the degree of strategic vulnerability it can generate for the State itself (Torreblanca 2021).

This logic responds to a scenario in which States prioritize relative gains over absolute gains. Historical experience shows that when this logic prevails, States are willing to sacrifice their own economic growth if doing so helps to curb, contain, or slow the technological–and by extension military–development of their strategic rivals. In parallel, they seek to reduce levels of interdependence deemed excessive or dangerous through strategies of selective decoupling, especially in critical technological sectors.

This helps explain three closely linked contemporary dynamics: first, the restrictions imposed by the US on the export of advanced technologies to China; second, the acceleration of China's strategy of technological autonomy; and third, the European Union's insistence on achieving so-called technological sovereignty.

The dominant geopolitical impulse today is characterized by growing securitization of technology. States no longer conceive technological innovation primarily as a factor of economic efficiency or social welfare, but as a strategic resource of power.

The most immediate historical parallel is the 1980s, when the Reagan administration sought to prevent the Soviet Union from accessing dual-use digital technologies to slow its economic and military development. We are thus entering a new technological Cold War with its own characteristics, in which control, access, and the denial of markets, data, and critical technologies occupy a central place in political and strategic debate.

The geopolitical instrumentalization of technology and digital interconnectivity has generated growing disputes around multiple strategic domains: critical digital infrastructures (such as 5G networks and submarine cables), essential raw materials (including rare earths), key industries (artificial intelligence, cloud computing, semiconductors), control of data flows and storage, as well as the definition of technical standards that will shape the future development of emerging technologies.

In this context, numerous States have begun to raise digital borders by adopting data localization policies, export controls on sensitive technologies, and restrictions on the mobility of scientific talent (Ferracane et al. 2018). Simultaneously, they seek to build technological spheres of influence with politically like-minded countries, with the goal of expanding and consolidating both their structural power and their regulatory and technological models (CEIP 2019).

Historically, the technologies associated with major revolutions–agricultural, industrial, or information–tended to spread relatively widely once their initial development phase had been overcome (Ding 2024). No State managed to deny others sustained access to technologies such as the steamship, electricity, or more recently nuclear energy for civilian or even military use. Even contemporary attempts to limit nuclear proliferation of a military nature have had only partial success and only for limited periods of time. By contrast, the current moment is characterized by an unprecedented trend toward fragmentation of the international technological system into at least two large differentiated and mutually incompatible blocs: one led by the US and another headed by China.

The United States has been a pioneer in developing an integrated technological ecosystem capable of covering virtually all critical layers: from space and satellite infrastructures to submarine cables, digital platforms, cloud services, and advanced artificial intelligence capabilities. To achieve full technological autonomy, Washington still depends on some strategic bottlenecks, such as advanced lithography for semiconductor manufacturing–dominated by the Dutch company ASML–or the extraction and refining of rare earths, essential for the technology and defense industries, which China has dominated for decades.

China, for its part, has pursued a deliberate, long-term strategy aimed at technological self-sufficiency. Through early identification of critical sectors and massive State-coordinated investments–combined with a highly effective strategy of industrial espionage–Beijing has managed to position itself ahead of the US in certain strategic technologies and significantly reduce its external dependence. Although the manufacture of advanced semiconductors remains its main area of vulnerability, China is clearly on a path of technological convergence in this domain.

As a result, both the US and China can now offer their partners and allies comprehensive technological solutions that exclude, wholly or partially, the rival bloc. Analogous to the construction of a "great digital wall" in China's internal market–by excluding the main US technology companies–Beijing has sought to expand its structural power by creating its own technological sphere of influence internationally.

These dynamics evoke the so-called "Great Game" of the nineteenth century between the British Empire and the Russian Empire, in which competition for spheres of influence combined strategic, economic, and technological interests. In the current context, technological alliances allow great powers to access new markets, raw materials, and data flows, while vying to impose their technical and normative standards globally (Hobbs et al. 2016; Walker 2022).

Consequently, although the technological revolution will continue advancing, its trajectory will no longer be guided exclusively by market logic, private economic actors, or multilateral institutions. On the contrary, governments have come to play a central role, steering technological development under criteria of national security, geopolitical competition, and strategic control, configuring an increasingly fragmented and competitive international system. From the aspiration of global interconnection, we have therefore moved to the reality of technological balkanization, decoupling, and the reduction of interdependencies and vulnerabilities (Leonard 2021).

TECHNOLOGY COERCION

The role of middle powers such as Brazil, the EU, India or Japan in an international system increasingly dominated by technological rivalries is profoundly problematic. By its very nature as a civil and normative power, the EU has historically tended to conceive of technology as an instrument of economic prosperity, social cohesion, and rights expansion, and not as a vector of geopolitical power. This approach has translated–especially over the last decade–into a strong bet on regulatory governance of technology centered on protecting fundamental rights, fair competition, and limiting abuses of power by private actors.

This strategy has earned the Union the label of "regulatory superpower," fuelling the expectation that it could consolidate itself as a third normative technological pole, alternative to the US and Chinese models. In this vision, Europe aspires to become an attractive space for those States and societies that defend a rules-based international order, with relatively open access to technology–where technology would not be a source of strategic coercion or structural dependence, but a multiplier of development, inclusion, and individual autonomy (Hobbs & Torreblanca 2020).

Through the so-called "Brussels effect," the EU has demonstrated a notable capacity to export its regulatory norms, especially in areas such as privacy and data protection. European regulations such as the General Data Protection Regulation (GDPR), which governs data privacy, came to be considered the "gold standard" of digital regulation worldwide. The size and attractiveness of the European market meant that even in the absence of major homegrown digital platforms, the leading US technology companies operated in Europe under significantly stricter standards than those prevailing in the US, where the absence of comprehensive federal privacy legislation has produced a much looser and more fragmented framework (Bradford 2020; 2023).

However, the implicit hypothesis that Europe could benefit from advanced digital services without developing equivalent industrial capabilities of its own has progressively eroded as geopolitical competition over technology between the US and China has intensified.

In a first phase, the United States successfully pressured the EU to decouple technologically from China, particularly in sectors such as 5G networks, depriving member States of relevant technological alternatives. In a second phase, Washington began to instrumentalize Europe's dependence on US technology to challenge European regulations and try to obtain exemptions or favorable reinterpretations for its companies. Finally, as Sino-American rivalry has sharpened, Washington has intensified pressure on Brussels to align its regulatory standards with US standards, characterizing European norms as extraterritorial, discriminatory, and even extortionate.

This dynamic has placed the EU in a position of structural vulnerability, lacking the material capacity needed to credibly evade coercion from either the US or China. The European strategy of developing indigenous technological alternatives in areas such as semiconductors, cloud, or artificial intelligence is a rational response, but extremely costly in time, financial resources, and political coordination. Consequently, this path cannot guarantee European technological sovereignty in the short term, forcing the EU to operate for a prolonged period under conditions of strategic dependence.

US pressure for Europe to reject Chinese technology began during the first Trump administration, but not only continued–it intensified–under the Biden administration, especially through the proliferation of export controls on critical technologies to China. According to the characterization of then National Security Advisor Jake Sullivan, the US would build a "small yard with high fences" in the technological domain (Biden 2023). However, the inclusion in these restrictions of the three most strategic technologies of the present–artificial intelligence, semiconductors, and quantum computing–made clear that this "yard" was far from small. On the contrary, it signalled the launch of a frontal challenge to China.

Another episode revealing Europe's vulnerability vis-à-vis the US occurred with the Dutch government's decision–directly in response to US pressure–to require ASML to cease exporting extreme ultraviolet lithography machines, indispensable for manufacturing advanced semiconductors. This case showed how even Europe's scarce critical technological advantages could be neutralized by external political decisions (Qin 2024).

Europe's dependence on private US technology companies became even more exposed during the war in Ukraine. In September 2022, Elon Musk ordered restrictions on Ukrainian access to the low-orbit satellite system Starlink, crucial for Ukrainian military communications (Roulette, Bryan-Low & Balmforth 2025). Musk justified his decision by claiming fear of nuclear escalation. This episode demonstrated the inherent risks of having technological capabilities essential to collective security controlled by private actors, capable of directly influencing strategic dynamics of the first order.

The Starlink case marked a turning point for the EU, revealing in tangible terms the consequences of having outsourced critical infrastructures to foreign private companies. Added to this were Musk's increasingly aggressive attacks on the EU during the US electoral cycle–also suffered by Brazil–, aligned with the positions of then President Donald Trump and the MAGA movement. These positions were reinforced by statements from then Senator J.D. Vance, who went so far as to question US commitment to Europe by alleging a supposed degradation of European democratic quality due to its digital regulations.

After his appointment as Vice President of the United States, Vance elevated this criticism to a central axis of US policy toward Europe in a controversial speech delivered at the Munich Security Conference in February 2025, in which he argued that the main threat to Europe did not come from Russia but from internal restrictions on freedom of expression (Vance 2025).

That same month, President Trump instructed his Secretaries of Commerce and the Treasury to respond to what he called European "regulatory extortions," referring directly to digital services and digital markets legislation (White House 2025a). Thus, the alliance between the White House and major US tech companies was made explicit–already visible at Trump's inauguration ceremony, attended by leading Silicon Valley executives. Figures such as Mark Zuckerberg have equated European regulation with institutionalized censorship systems comparable–according to him–to those of China. Both Zuckerberg and Musk have openly challenged the Union, refusing to comply with certain obligations related to combating disinformation and online harms on platforms such as X.

Musk's direct interference in European political processes–such as his explicit support for anti-system forces like Alternative for Germany (AfD) during the German legislative elections in February 2025–has had a notable political impact. Not only for backing an extremist force, but for normalizing narratives that relativized Germany's historical past, which has been perceived as unprecedented interference by a foreign private actor.

A new source of alarm emerged with the Trump administration's decision to impose sanctions on the International Criminal Court after it issued arrest warrants against Israeli Prime Minister Benjamin Netanyahu: the US forced Microsoft to withdraw email services from the prosecutor responsible for the case. The company complied, showing that under US law companies must comply first and litigate later–even when this affects international institutions based in Europe (Satariano & Smialek 2025).

This episode highlighted unequivocally the systemic risk derived from Europe's dependence on US cloud computing services. Although it reinforced interest in developing European sovereign cloud infrastructures, it also confirmed that such alternatives would not be available in the short term, thus prolonging Europe's exposure to potential political coercion.

Finally, the publication of US national security doctrine in December 2025 confirmed Europe's worst fears by openly legitimizing the instrumentalization of US technological superiority for purposes of political transformation in Europe. The US strategy describes Europe as the victim of an anti-democratic ideological drift and defends the need to promote access to power for political forces aligned with Trumpism. The fear, from the European perspective, is that the US will replicate–through private digital platforms–influence tactics like those previously used by Russia, provoking a frontal transatlantic clash over digital services, regulatory sovereignty, and democracy (White House 2025b).

Taken together, these episodes reveal that the EU faces not only a deficit of technological capabilities, but an existential challenge in terms of sovereignty and democracy, in a context in which technology has ceased to be a neutral good and has become a central instrument of geopolitical coercion.

DEMOCRACY AND SOVEREIGNTY

The EU has explicitly recognized that technology constitutes a central dimension of its security and political autonomy (European Commission 2023). The European Commission that emerged from the June 2024 elections materializes this recognition by creating, for the first time, an Executive Vice Presidency dedicated to Technological Sovereignty–marking a turning point in Europe's conception of power in the twenty-first century.

Although the concept of technological sovereignty is not univocal–and is especially complex in a global context characterized by deep interdependencies and cross-cutting vulnerabilities–European institutions use it to refer to a concrete idea:

the Union's ability to make digital and technological decisions in accordance with its own interests and values, without being subject to external coercion deriving from critical dependencies.

From this perspective, guaranteeing European technological security requires acting simultaneously on four complementary planes: in-house capabilities, resilience against coercion, defense of the democratic space; and international alliances partnerships.

The first pillar–inevitable but long-term–consists of developing a European technological and industrial base (Eurostack) in those areas where external dependence generates economic or security risks. The mission letter sent by the President of the Commission, Ursula von der Leyen, to the head of the new portfolio clearly identifies these sectors: supercomputing, semiconductors, cloud computing, artificial intelligence, quantum computing, space technologies, the Internet of Things, and genomics (von der Leyen 2024).

Without its own capabilities in these areas, the EU lacks real room for manoeuvre. Technological security cannot rest exclusively on regulation if there is no material infrastructure that can provide credible alternatives. However, this strategy requires massive investments, coordination among member States, and explicit political acceptance that industrial policy is an unavoidable national security necessity.

Second, because development of these capabilities will take years, the EU needs instruments of protection and deterrence in the short- and medium-term against technological coercion by third parties, including its allies. Recent experience shows that Europe's dependence on US digital technologies and services can be used as a lever for political, regulatory, or even ideological pressure.

To mitigate this vulnerability, the Union should adopt a strategy that, first, uses trade policy strategically, recalling that the US maintains a structural surplus with the EU in digital services; second, strengthens competition policy by reducing the market power–and by extension the political power–of major technology platforms; third, advances common fiscal instruments, indispensable for financing strategic technological investments and avoiding regulatory capture; and fourth, explores national security tools, including European preference clauses or selective restrictions in sectors considered critical.

These instruments have already been applied with respect to China, to reduce dependence on companies from that country subject to legal frameworks that compel them to cooperate with intelligence services. Given that the US has comparable legislation with extraterritorial effects, the EU must also begin to assess the security

risk stemming from exposure to US companies, especially in areas such as cloud services, digital platforms, or data infrastructures.

A third element of European technological security is defending democratic processes against digital interference. The EU has made significant progress in this area through the Digital Services Act and the Digital Markets Act, as well as by adopting the so-called "democratic shield," which explicitly recognizes electoral processes as critical infrastructures comparable to energy or transport infrastructures.

This approach is essential in a context in which digital platforms–whether US or Chinese–can be used as vehicles for disinformation, information manipulation, or indirect support for political forces hostile to democracy. Guaranteeing technological security therefore implies guaranteeing the integrity of public debate, even against private actors with systemic influence capacity.

As Brazil experiences, other middle and regional powers are also exposed to technological coercion and to foreign interference in democratic processes, often amplified by poorly regulated online platforms. These States therefore must cooperate in protecting democracy and sovereignty.

Despite its vulnerability in other areas, the EU has shown that it should not give up its regulatory power. Effective enforcement of European digital legislation against major technology companies–including sanctions for non-compliance–constitutes one of the few instruments of structural power available to the EU. Conceding on this terrain would not reduce external pressure; it would increase it, by confirming that technological dependence can translate into political subordination. Regulatory firmness is not incompatible with transatlantic cooperation; it is in fact a condition for such cooperation to be based on more symmetrical relations (Torreblanca 2025).

Fourth. The EU is not the only democracy whose access to critical technologies may be constrained by US-China competition. As Brazil experiences, other middle and regional powers are also exposed to technological coercion and to foreign interference in democratic processes, often amplified by poorly regulated online platforms. These States therefore must cooperate in protecting democracy and sovereignty. These goals are best pursued through regional and global cooperation to uphold a rules-based, open, human-centered technological order. Initiatives such as the EU-Latin America and Caribbean Digital Alliance,

and the AI regulatory coordination work of the OECD, the G7, and the G20, show the way ahead (Torreblanca et al. 2025).

In a world in which only two major technological poles exist–the US and China–the EU faces the risk of becoming a digital colony if it does not act decisively. Paradoxically, its vulnerability today is greater vis-à-vis the US than vis-à-vis China, precisely because of the depth of existing interdependence. Guaranteeing European technological security therefore requires a combination of ambitious industrial policy, instruments of defense against coercion, protection of the democratic space, and sustained political will. Technological sovereignty is not an end in itself; it is the necessary condition for preserving Europe's political, economic, and social model in an increasingly competitive and coercive international environment.

CONCLUSION

Technology has become a central factor of international power, comparable to territory, population, or strategic resources. The current technological revolution–characterized by its speed, global reach, and the structural role of private actors–is accelerating the securitization of innovation and pushing the international system toward a logic of rivalry, fragmentation, and competition between technological blocs led by the United States and China.

In this context, the EU occupies an ambivalent position. Its strength as a regulatory power has enabled it to influence global digital governance, but the lack of its own industrial capabilities in critical technologies exposes it to dependencies that already translate into extreme vulnerability to external coercion.

Regulation alone is not sufficient to defend European sovereignty in an increasingly hostile geopolitical environment. Guaranteeing European technological security therefore requires an integrated strategy that combines long-term industrial policy, instruments of resilience and deterrence against technological coercion, and strengthened protection of the democratic space against digital interference.

Technological sovereignty is the necessary condition for preserving the EU's decision-making capacity, democratic model, and strategic autonomy in the international order of the twenty-first century.

References

Allison, Graham. 2017. *Destined for War: Can America and China Escape Thucydides's Trap?* Houghton Mifflin Harcourt.

BBC News. 2020. "Huawei Ban: UK o Impose Early End o Use of New 5G Kit." November 29, 2020. https://www.bbc.com/news/business-55124236.

Biden, Joseph R. 2023. "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution." *The American Presidency Project*, April 27, 2023. https://www.presidency.ucsb.edu/node/360988.

Biden, Joseph R. 2025. "President Biden's Farewell Address." *The White House*, January 15, 2025. https://www.whitehouse.gov/briefing-room/speeches-remarks/2025/01/15/remarks-by-president-joe-biden-in-farewell-address-to-the-nation/.

Bradford, Anu. 2020. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001.

Bradford, Anu. 2023. *Digital Empires: The Battle for Global Tech Dominance*. New York: Oxford University Press.

Bria, Francesca. 2025. "El golpe de Estado de los tecnoautoritarios: de la América postdemocrática a la Europa que viene." *La Vanguardia*, November 2, 2025. https://www.lavanguardia.com/internacional/20251102/11220880/golpe-tecnoautoritarios-america-postdemocratica-europa-viene.html.

Ding, Jeffrey. 2024. *Technology and the Rise of Great Powers: How Diffusion Shapes Economic Competition*. Princeton University Press.

European Commission. 2023. "Joint Communication on 'European Economic Security Strategy'." *High Representative of the Union for Foreign Affairs and Security Policy*, June 20, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020

Feldstein, Steve. 2019. "The Global Expansion of AI Surveillance." *Carnegie Endowment for International Peace*, September 17, 2019. https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en.

Ferracane, Martina Francesca, Hosuk Lee-Makiyama & Erik van der Marel. 2018. *Digital Trade Restrictiveness Index*. Brussels: European Centre for International Political Economy (ECIPE). https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf.

Frías Sanchéz, Carlos Javier. 2024. "Rusia, Ucrania y el campo de batalla 'transparente'." *Documento de Opinión* 18/2024, Instituto Español de Estudios Estratégicos (IEEE). https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO18_2024_CARFRI_Rusia.pdf.

Headrick, D. R. 1979. *Los instrumentos del imperio: tecnología y colonialismo europeo en el siglo XIX*. Madrid: Alianza.

Hobbs, Carla, & José Ignacio Torreblanca. 2020. *La soberanía digital de Europa.* Madrid: Catarata.

Hobbs, Carla, Andrew Puddephatt & José Ignacio Torreblanca. 2016. "The Geoeconomics of the Digital." In *Connectivity Wars: Why Migration, Finance and Trade Are the Geo-Economic Battlegrounds of the Future*, Mark Leonard (ed): 110-118. https://ecfr.eu/archive/page/-/Connectivity_Wars.pdf.

Hu, Krystal. 2023. "ChatGPT Sets Record for Fastest-Growing User Base in History." *Reuters*, February 1, 2023. https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/.

Kissinger, Henry A., Eric Schmidt & Daniel Huttenlocher. 2021. *The Age of AI: And Our Human Future*. New York: Little, Brown & Company.

Leonard, Mark. 2021. *The Age of Unpeace: How Connectivity Causes Conflict*. London: Bantam Press.

Qin, Sherry. 2024. "Netherlands Blocks ASML Exports of Some Chip-Making Equipment to China." *Wall Street Journal*, January 2, 2024. https://www.wsj.com/tech/netherlands-blocks-asml-exports-of-some-chip-making-equipment-to-china-2fe4a162.

Roulette, Joey, Cassell Bryan-Low & Tom Balmforth. 2025. "Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia." *Reuters*, July 25, 2025. https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/.

Satariano, Adam & Jeanne Smialek. 2025. "Europe's Growing Fear: How Trump Might Use US Tech Companies Against Europe." *The New York Times*, June 20, 2025. https://www.nytimes.com/2025/06/20/technology/us-tech-europe-microsoft-trump-icc.html.

Torreblanca, José Ignacio & Irene Sánchez. 2023. "Ukraine One Year on: When Tech Companies Go to War." *European Council on Foreign Relations*, March 7, 2023. https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/.

Torreblanca, José Ignacio, Ángel Melguizo, Irene Sánchez, Manuel Acevedo & Víctor Muñoz. 2025. "Connecting Regions, Closing Gaps, Building Sovereignty. The European Union-Latin America and the Caribbean Digital Alliance: Recommendations for the EU-CELAC Summit." *Occasional Paper Fundación Carolina/ECFR*. https://doi.org/10.33960/issn-e.1885-9119.DTFCECFRen.

Torreblanca, José Ignacio. 2020. "Democracia y redes sociales." In *Cómo salvar las democracias liberales*, Víctor Lapuente & Esther Costas (eds): 131-150. https://hdl.handle.net/20.500.14468/25563.

Torreblanca, José Ignacio. 2021. "Technology." In *The Power Atlas: Seven Battlegrounds of a Network World*, European Council on Foreign Relations: 38-61. https://ecfr.eu/wp-content/uploads/power-atlas.pdf.

Torreblanca, José Ignacio. 2025. "Big Tech, Donald Trump, and Techno-imperialism: How Europe Can Avoid Becoming a Digital Colony." *European Council on Foreign Relations*, January 20, 2025. https://ecfr.eu/article/big-tech-donald-trump-and-techno-imperialism-how-can-europe-avoid-becoming-a-digital-colony/.

Vance, J. D. 2025. "Speech at the Munich Security Conference." *Munich Security Report*, February 14, 2025. https://securityconference.org/en/medialibrary/asset/the-speech-of-jd-vance-20250214-1817/.

von der Leyen, Ursula. 2024. "Mission Letter." *European Commission*, September 17, 2024. https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf.

Walker, Justine. 2022. "US Hits China with Sweeping Tech Export Controls." Financial Times, October 7, 2022. https://www.ft.com/content/6825bee4-52a7-4c86-b1aa-31c100708c3e.

White House. 2025a. "Memorandum on Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties." *The White House*, February 21, 2025. https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/.

White House. 2025b. *National Security Strategy of the United States of America*. Washington, DC: The White House. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

Como citar: Torreblanca, José Ignacio. 2025. "Defendendo a democracia e a soberania na União Europeia diante da nova geopolítica da tecnologia". *CEBRI-Revista* Ano 4, Número 16 (Out-Dez): 155-173.

To cite this work: Torreblanca, José Ignacio. 2025. "Defending EU Democracy and Sovereignty from the New Geopolitics of Technology." *CEBRI-Journal* Year 4, No. 16 (Oct-Dec): 155-173.

DOI: https://doi.org/10.54827/issn2764-7897.cebri2025.16.02.11.155-173.en

Submitted: January 28, 2026
Accepted for publication: March 3, 2026