Instituto Español de Estudios Estratégicos

Analysis
Paper

40/2026 19/05/2026

José Ignacio Torreblanca

Power, Geopolitics, Sovereignty and Technology

Visit webpage Receive Newsletter

Power, Geopolitics, Sovereignty and Technology

This analysis is part of the Strategy Notebook:
Strategic Panorama 2026. *Published in March 2026*

Abstract:

This text examines the return of technology as a structural variable of international power. It argues that, just as in previous revolutions—the agricultural, industrial and digital ones—contemporary technological innovations are reshaping the economy, state organisation and the global order. However, it shows that the current technological revolution has distinctive features: rapid and global diffusion, the consolidation of the digital sphere as a domain of conflict, and the emergence of private companies as providers of infrastructures that are essential to sovereignty and security.
The competition between the US and China, the text argues, is driving dynamics of securitisation, selective decoupling and fragmentation into technological blocs, with direct consequences for standards, data, supply chains and alliances. Finally, the text examines the European Union's vulnerable position: strong in regulatory capacity, yet dependent on and exposed to the United States and China for access to critical technologies. On the basis of this diagnosis, it calls for the construction of European digital sovereignty as a prerequisite for preserving the EU's strategic autonomy, its democratic and values-based model, and its capacity for political and strategic decision-making.

Keywords: Digital sovereignty, Geopolitics of technology, Technological coercion, Artificial intelligence, European digital regulation.

How to cite this document:

TORREBLANCA, José Ignacio. *Power, Geopolitics, Sovereignty and Technology*. Documento de Analysis Paper IEEE 40/2026. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introduction

This text examines the return of technology as a structural variable of international power. It argues that, just as in previous revolutions—the agricultural, industrial and digital ones—contemporary technological innovations are reshaping the economy, state organisation and the global order. However, it shows that the current technological revolution has distinctive features: rapid and global diffusion, the consolidation of the digital sphere as a domain of conflict, and the emergence of private companies as providers of infrastructures that are essential to sovereignty and security.

The competition between the US and China, the text argues, is driving dynamics of securitisation, selective decoupling and fragmentation into technological blocs, with direct consequences for standards, data, supply chains and alliances. Finally, the text examines the European Union's vulnerable position: strong in regulatory capacity, yet dependent on and exposed to the United States and China for access to critical technologies. On the basis of this diagnosis, it calls for the construction of European digital sovereignty as a prerequisite for preserving the EU's strategic autonomy, its democratic and values-based model, and its capacity for political and strategic decision-making.

The return of history

At present, the major powers, fully aware that access to, control of and mastery of critical technologies are indispensable requirements for their strategic survival, have entered into an increasingly intense competition to secure their digital and technological sovereignty. This rivalry is not limited to the economic sphere, but encompasses military, political, cultural and regulatory dimensions. Technology has thus become a structural factor in power and international rivalry, on a par with territory, population, or natural resources.

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 the relations between its units. These changes have often led to major conflicts, both within and between states.

Around seven thousand years ago, the transition from subsistence economies to forms of intensive agriculture, associated with the domestication of species such as wheat and

the development of irrigation technologies, brought about a radical change in social organisation. The generation of agricultural surpluses enabled the specialisation of labour and laid the foundations for the emergence of the first permanent political institutions: administrative bureaucracies, tax systems, professional armies and religious hierarchies.

These advances fostered the codification of law, the formal organisation of knowledge and the expansion of long-distance trade. At the same time, the need to manage large populations and territories favoured a concentration of political power in specific geographical centres, giving rise to complex state structures. Thus emerged the so-called “hydraulic empires”, whose power rested on the control of water and agricultural resources, as well as on the ability to finance and arm large armies. These entities projected their influence beyond their borders, coming into conflict with similar political entities.

Closer to our own time, the First Industrial Revolution (1760–1840), driven by the steam engine, the mechanisation of the textile industry and the intensive use of coal, also had profound political and geopolitical consequences. On the one hand, it marked the decisive shift from an agrarian to an industrial economy. On the other, it eroded the political, social and economic structures of the *Ancien Régime*, facilitating the transition towards economic and political liberalism. Industrialisation accelerated urbanisation and gave rise to new social classes—the industrial bourgeoisie and the urban proletariat—whose demands profoundly transformed the structures of political representation.

These changes triggered political revolutions—the American (1776–1789) and the French (1789–1808)—which crystallised in new forms of state organisation that challenged the traditional European monarchical order and profoundly altered the international order prevailing at that time. The clash between these new regimes and the absolute monarchies led to a prolonged period of armed conflict that culminated in the Congress of Vienna (1814) and the creation of a new continental balance of power.

Similarly, the Second Industrial Revolution (1860–1930), based on electricity, the railway, the telegraph and steamships, greatly amplified the states” capacity to project power, both domestically and internationally. These technologies drastically reduced transport and communication costs, integrating national markets and expanding global trade on an unprecedented scale.

The geopolitical impact of Western technological superiority was a decisive factor, as it enabled the domination of vast territories at a relatively low cost. Just as Spanish expansion in the Americas had relied on advances in navigation, metallurgy and the use of the horse, the conquest of Africa in the 19TH century and the great era of colonialism that followed would have been unthinkable without the technological trident formed by the steamship, the machine gun and quinine (Headrick, 1979). Technology not only conferred military advantages but also gave rise to a system of international relations based on the creation of large colonial empires and the rivalries between them. Although the European empires succeeded in dominating Asia and Africa—and the United States, in the light of the Monroe Doctrine revived today, the American continent—the clash between the European empires led to the First World War and the beginning of a long process of European decline.

In Asia, the cases of China and Japan clearly illustrate the consequences of technological backwardness. During the 19TH century, the Qing Empire's inability to adopt the key technologies of the Industrial Revolution led to a series of military defeats at the hands of Western powers, culminating in the Opium Wars and the so-called "Century of Humiliation". This historical experience has left a lasting mark on Chinese strategic culture. The central importance that Chinese leaders now assign to technology as a guarantor of national sovereignty and international status cannot be understood without this historical background. Their determined effort not to fall behind in fields such as artificial intelligence, advanced computing, or semiconductors responds as much to economic calculations as to geopolitical and survival logic.

Similarly, Japan, which during the Tokugawa period had maintained a policy of international isolation, suffered a major technological shock with profound political, economic and cultural consequences in 1853 following the arrival of the American "black ships" — as Commodore Perry's steam-powered vessels were known — and was also forced to sign a series of completely asymmetrical treaties that compelled it to open up to international trade.

The Third Industrial Revolution (1970–2000), centred on information and communication technologies (ICT), has also brought about structural changes to economies and states. At the end of the last century, digitalisation, automation and financial liberalisation facilitated a new wave of globalisation, characterised by transnational value chains,

massive capital flows and unprecedented market integration. These dynamics favoured the emergence of major new international players, particularly China, but also other countries in the Global South, a phenomenon accelerated by the end of the Cold War and the integration of China, India and other Asian economies into the dynamics of globalisation.

The diffusion of technological progress and innovation from the West to the rest of the world has resulted in the gradual erosion of Western dominance and the transition towards a multipolar international order in which economic and technological power is more diffusely distributed. Within this dynamic, China's rise has led to the emergence of a power capable of competing economically, technologically and militarily with the US. This has prompted analysts to consider the possibility of conflict between the two powers in accordance with historical patterns observed between established and rising powers, referred to in terms of the "Thucydides Trap" by authors such as Allison (2017), who identified sixteen major power transitions throughout history, concluding that only four did not result in armed conflict.

The Fourth Industrial Revolution, which began around 2010 with advances in robotics, global connectivity and artificial intelligence, is deepening these transformations in an even more distinctive manner. The centre of gravity of corporate power has shifted from traditional sectors—such as energy or finance—towards the technology sector, which ranges from cloud software and semiconductors to critical digital infrastructure and social media platforms and networks.

This shift has led to increasing state intervention in areas previously considered predominantly private. Major powers now compete to control the strategic nodes of the digital economy: data, algorithms, connectivity infrastructure and computing power. In this context, artificial intelligence has become a central arena of geopolitical rivalry, particularly between the US and China, with direct implications for alliances, international norms and balances of power. AI is not only transforming productive and labour relations within states, but is also reshaping the architecture of global power by introducing new technological asymmetries and dependencies. As in previous technological revolutions, those who succeed in mastering these capabilities will largely define the rules of the international order of the twenty-first century and the hierarchy of power within it.

Whereas in the 1980s the world's largest companies by market capitalisation were the major oil or banking firms, today that position is occupied by major US tech firms such as Nvidia, Google, Amazon, Apple and Meta, with Chinese tech firms trailing far behind and no significant presence of European companies among the world's twenty largest. This corporate landscape today maps out the distribution of global economic and technological power, but also a new geopolitics so profoundly shaped by the transformation of interdependencies into vulnerabilities (Leonard, 2021), asymmetries in technological capabilities and connectivity wars, just as the second half of THE 20TH century was shaped by asymmetries surrounding access to oil and gas.

The international consequences of this reshaping of the world around digital technologies are clear. Just as the economy based on the exploitation of fossil fuels gave rise to an international order and a series of alliances linked to access to and control of production centres in the Middle East and the Persian Gulf, the current data-driven economy is generating its own system of international relations, based on access to critical raw materials necessary to sustain technological development and to the supply chains, production centres, and distribution networks of digital technologies — particularly Taiwan. For Europe, the new geopolitics of technology implies a transition from dependencies and vulnerabilities associated with oil and gas from the Middle East and Russia to becoming trapped in a new dependence on artificial intelligence models, data centres, semiconductors, and other technologies contested between the United States and China.

The new geopolitics of technology

As highlighted in the previous section, technological innovations have repeatedly brought about profound transformations both within states and within the international system, altering power relations, forms of political organisation, and the dynamics of conflict and cooperation. However, and despite the clear continuities between the current technological revolution and previous historical processes, it is possible to identify a series of qualitatively novel elements that distinguish contemporary technological transformation from preceding revolutions.

First, it is worth noting the speed, scope and depth of current technological changes, particularly with regard to global connectivity and the dissemination of innovations. Whilst key 20TH century technologies, such as the telephone, took nearly half a century to reach one million users and a century to reach 100 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). This phenomenon is not exceptional, but rather representative of a broader dynamic: the spread of new technologies no longer follows gradual patterns, but rather accelerated and simultaneous processes on a global scale.

A similar transformation can be observed in the economic sphere. Historically, the expansion of international trade was constrained by physical, technological and regulatory barriers, advancing progressively and in waves linked to improvements in transport and communications. In contrast, trade in digital services lacks these material constraints, which has enabled technology companies to scale their business models extremely rapidly and operate simultaneously in multiple national markets. This feature reinforces the concentration of economic and technological power in a limited number of players—particularly American ones—capable of exploiting global economies of scale.

A second novel element concerns the transformation of the concept of security brought about by technological development. Alongside the traditional domains of warfare—land, sea, air and space—a fifth operational domain has emerged: cyberspace, which encompasses not only attacks on critical infrastructure, with increasing potential due to the growing connectivity of devices (*the Internet of Things*), but also the manipulation of the informational or cognitive domain.

In this domain, both defensive and offensive operations are conducted that can seriously affecting states" ability to act. These actions may have a direct material impact, by degrading or rendering military systems, critical infrastructure or command and control networks inoperable, but also a psychological and social impact, through disinformation campaigns, information manipulation and influence operations aimed at eroding social cohesion and the will to resist among the rulers and civilian population of a state, often making use of agents of influence or local political forces that amplify such content.

Authoritarian regimes, particularly Russia and China, have found the openness and lack of regulation of social media platforms in the West to be a highly effective tool for consolidating their power, both domestically and internationally. As Margarita Simonyan,

director of Russian state media, pointed out, *Russia Today*, *Sputnik* and the global network of Russian media exist for the same reason that the Russian Ministry of Defence exists: to wage information warfare against the West, creating and captivating audiences which, as was evident immediately prior to the invasion of Ukraine, can be mobilised at critical junctures (Torreblanca, 2020).

The US experience during the 2016 presidential election clearly illustrates the destabilising potential of operations combining cyberattacks and disinformation. The hack of the Democratic Party's servers, coupled with the mass exposure of the population—estimated at up to 136 million people—to fake news amplified political polarisation and internal social divisions (Taylor, Ewing and Johnson, 2018).

Similarly, in the European context, from 2014 onwards, following the first invasion of Ukraine, Russia exploited the openness of social media, the weakness of traditional media and the vulnerability of public opinion to false or biased information to launch massive disinformation campaigns aimed at weakening and dividing European democracies.

Such interference was particularly visible during processes such as the 2016 referendum on the United Kingdom's membership of the EU (Brexit), but also in Spain. In our country, the events surrounding the illegal attempt at secession in Catalonia in 2017 highlighted how the most serious external threat to national sovereignty experienced by Spain in its recent democratic history did not take the form of conventional military action, but rather materialised through a widespread disinformation and foreign influence operation attributed to Russia. With the aim of weakening the EU and NATO by encouraging within Spain a phenomenon similar to the colour revolutions and the pro-democracy protests within Russia—which it believed the West had instigated— Moscow created a comprehensive disinformation ecosystem comprising official media outlets, strategic alliances with separatists, manipulation of social media, and the mobilisation of *proxies* with influence on both the far right and the far left (Alandete, 2017; Fernández, 2024; Schwirtz and Bautista, 2021; and Washington Post, 2017).

Disinformation phenomena, which intensified during the pandemic, leading the WHO to speak of an "infodemic", 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 the current technological revolution is the central role of private technology companies as providers of essential services for national sovereignty. Whereas in earlier historical periods strategic sectors such as banking, insurance, rail transport or the automotive industry were often privately owned, they could, at least in theory, be replicated or nationalised by the state in emergency situations.

During the Second World War, for example, civilian industrial capacities were converted relatively quickly for military purposes, as was the case with the automotive and aviation industries. Today, however, a substantial part of the critical infrastructure underpinning the functioning of advanced economies is in the hands of private companies, without the state having the technical, financial or temporal capacity to replace them. This is the case with cloud computing services, advanced semiconductor manufacturing, the deployment and maintenance of submarine communications cables, and low-orbit satellite networks. These infrastructures are crucial for both economic activity and military and intelligence capabilities, but they far exceed the direct productive capacities of the public sector (Sánchez and Torreblanca, 2023).

The conflict in Ukraine has brought this new reality into sharp relief. Western technology companies, particularly American ones such as Microsoft, Amazon and Starlink, have played a key role in safeguarding Ukraine's critical digital infrastructure, providing essential services to its armed forces—especially in relation to data acquisition and processing—and mitigating Russian cyberattacks. The growing fusion between the US Pentagon and certain software and digital services companies specialised in the military domain, such as Anduril or Palantir, paints a highly concerning picture. Just as Eisenhower had warned in 1953 about the power of what he called the "military-industrial complex", this concern over the structural power of private companies and their links to national sovereignty led President Biden to issue a similar warning in his farewell address regarding the "tech-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 tech companies (Biden, 2025; Bria, 2025).

As would be demonstrated from the inauguration of President Trump in January 2025 and in the months that followed, major American technology companies were able, with little effort, to ensure that the White House adopted as its own their longstanding grievances and demands against European legislation on digital services and markets,

leading to a direct confrontation and a series of open coercive measures against the EU—and, notably, also against the United Kingdom.

All these transformations have profound implications for international security. Traditionally, technological evolution and military doctrine tended to advance more or less in parallel, allowing states and their armed forces sufficient time to adapt their organisational structures, strategies and defence industries. In the current context, however, the pace of technological innovation far exceeds the planning, procurement and deployment cycles of military capabilities, whose time horizons are necessarily longer. As a result, technological acceleration introduces high levels of strategic uncertainty, making it difficult to anticipate threats and formulate stable doctrines.

Henry Kissinger drew attention to this problem in one of his most recent works (Kissinger, Schmidt and Huttenlocher, 2021). The post-Second World War international order was stabilised by the existence of the nuclear weapon, which not only established a clear and widely recognised hierarchy of power but also allowed for the development of a rational, explicit and shared theory of deterrence, regardless of ideological differences between actors. The possession of nuclear weapons, which was 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 constructing 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 for 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, capable of being employed unilaterally and by surprise to launch pre-emptive strikes. This characteristic 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 framework for deterrence and international governance capable of stabilising its use and preventing dynamics of uncontrolled escalation. Without a theory of deterrence adapted to this new technological reality, the

risk is not a lack of balance, but the creation of a structurally more unstable international order.

In a historical trajectory marked by the interactions between technology and the international order, artificial intelligence—although it is progressively reshaping the power relations and hierarchies between states and the international order itself, centred on a bipolar competition between the US and China, which can undoubtedly be described as "digital" (Bradford, 2023), has not yet brought about a decisive rupture that would allow for a conclusive definition of the new characteristics of global power or its elements of stability or instability.

Decoupling, the Cold War and technological spheres of influence

The dominant geopolitical trend today is characterised by an increasing securitisation of technology. States no longer view technological innovation primarily as a factor of economic efficiency or social welfare, but as a strategic resource of power. Consequently, every technological advance is assessed according to two central criteria: the relative power it may confer on third parties and the degree of strategic vulnerability it may generate for the state itself (Torreblanca, 2021).

This logic reflects a scenario in which states prioritise relative gains over absolute gains. Historical experience shows that, when this logic prevails, states are willing to sacrifice their own economic growth if this helps to curb, contain or slow down the technological—and, by extension, military—development of their strategic rivals. At the same time, they seek to reduce levels of interdependence deemed excessive or dangerous through strategies of selective decoupling, particularly in critical technology sectors.

This analytical framework 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 for technological autonomy; and third, the EU's insistence on achieving so-called digital sovereignty.

The closest historical parallel lies in the 1980s, when the Reagan administration sought to prevent the Soviet Union from accessing dual-use digital technologies with the aim of slowing its economic and military development. We are thus entering a new technological cold war with its own distinct characteristics, in which control, access and denial of

markets, data and critical technologies occupy a central place in the political and strategic debate.

The geopolitical instrumentalization of technology and digital interconnectivity has generated growing disputes across multiple strategic areas: critical digital infrastructure (such as 5G networks and submarine cables), essential raw materials (including rare earths), key industries (artificial intelligence, cloud computing, semiconductors), the 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 erect digital borders, adopting data localisation policies, controls on the export of sensitive technologies and restrictions on the mobility of scientific talent (Ferracane, Marel and Lee-Makiyama, 2018). At the same time, they seek to build spheres of technological influence with countries considered politically aligned, with the aim of expanding and consolidating both their structural power and their regulatory and technological models.

Historically, technologies associated with major revolutions—agricultural, industrial or informational—tended to spread relatively widely once their initial phase of development had been overcome (Ding, 2024). No state has managed to consistently deny others access to technologies such as the steamship, electricity or, more recently, nuclear energy for civilian or even military use. Even contemporary attempts to limit the proliferation of nuclear weapons have had only partial and temporary success.

During the Cold War, although the Western bloc sought to restrict the Soviet bloc's access to certain technologies, the global technological ecosystem remained essentially unified. The major powers developed comparable military technologies, involving extensive copying, espionage and adaptation. By contrast, the present moment is characterised by an unprecedented trend towards the fragmentation of the international technological system into at least two large, differentiated and incompatible blocs: one led by the United States and the other by China.

The US has pioneered the development of an integrated technological ecosystem, capable of covering virtually all critical layers: from space and satellite infrastructure to undersea cables, digital platforms, cloud services and advanced artificial intelligence capabilities. To achieve full technological autonomy, Washington still relies on certain

strategic bottlenecks, such as advanced lithography for semiconductor manufacturing—dominated by the Dutch firm ASML—or the extraction and refining of rare earths, essential for the technology and defence industries, which China has dominated for decades.

China, for its part, has deployed a deliberate, long-term strategy aimed at technological self-sufficiency. Through the early identification of critical sectors and massive state-coordinated investment, combined with a highly effective industrial espionage strategy, 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 on a clear path towards technological convergence in this field.

As a result, both the US and China are now in a position to offer their partners and allies comprehensive technological solutions that exclude, either wholly or partially, the rival bloc. In a manner analogous to the construction of a “great digital wall” in the Chinese domestic market — through the exclusion of major US technology firms — Beijing has sought to expand its structural power by creating its own sphere of technological influence on an international scale.

These dynamics evoke the so-called “Great Game” of the 19TH 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 enable major powers to access new markets, raw materials and data flows, whilst striving to impose their technical and regulatory standards globally (Hobbs, Puddepath and Torreblanca, 2016; Financial Times, 2022).

According to available data, China has exported surveillance technologies to more than sixty countries, including Iran, Myanmar, Venezuela and Zimbabwe, many of which have serious human rights deficits (Feldstein, 2019). Thirty-six of these countries are part of the Belt and Road Initiative, which facilitates their access to concessional financing to acquire technologies from Chinese companies such as Huawei, Hikvision, Dahua and ZTE. In other emerging fields, such as blockchain, Beijing has promoted initiatives such as the Blockchain-Based Service Network (BSN) with the aim of reshaping the global digital architecture and creating infrastructures based on standards defined by China. At the same time as it exports technology, China imports critical raw materials to sustain its

technological development, generating extractive relationships and processes of economic re-primarisation that resemble a new form of digital colonialism.

Liberal democracies have not remained outside these dynamics. In addition to using and exporting surveillance technologies, they have promoted digital alliances aimed at limiting the expansion of Chinese technological power. A significant example was the Clean Network Initiative, promoted during the first Trump administration by the then Secretary of State, Mike Pompeo, which sought to encourage US allies to restrict the use of Chinese technologies and adopt what were termed “clean” infrastructures in areas such as networks, applications, cloud services, cables and data routes (BBC News, 2020).

This group included EU member states, along with Asian allies such as Japan, Israel, Australia, Canada, India and New Zealand, as well as Latin American nations, and explicitly invoked Cold War-style containment strategies. Gradually, in Europe, Latin America and other regions, numerous countries have begun to distance themselves from Chinese suppliers, considered “high-risk”, whilst China has intensified its efforts to replace Western technologies with domestic solutions in its own market.

Technological competition is also expressed through the increasing use of foreign influence operations, disinformation and cyberattacks, which have become central instruments of contemporary hybrid warfare. These practices have encouraged many states to reduce their level of digital interconnection and even to fragment the internet and their technological industrial bases in order to limit strategic dependencies.

Consequently, although the technological revolution will continue to advance, 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 according to criteria of national security, geopolitical competition and strategic control, shaping an increasingly fragmented and competitive international system. We have thus moved from the aspiration of global interconnection to the reality of technological balkanisation, decoupling and the reduction of interdependencies and vulnerabilities.

The EU: from regulatory superpower to digital colony

The role of the European Union in an international system increasingly dominated by technological rivalries is deeply problematic. By its nature as a civilian and normative power, the EU has historically tended to conceive technology as an instrument of economic prosperity, social cohesion and the expansion of rights, rather than as a vector of geopolitical power. This approach has translated, particularly over the past decade, into a strong commitment to a regulatory governance of technology centred on the protection of fundamental rights, fair competition and the limitation of abuses of power by private actors.

This strategy has earned the Union the label of a “regulatory superpower”, fostering the expectation that it might consolidate itself as a third normative technological pole, alternative to the American and Chinese models. In this vision, Europe aspires to become an attractive space for those states and societies that support a rules-based international order, with relatively open access to technology, where technology is not a source of strategic coercion or structural dependency, but a multiplier of development, inclusion and individual autonomy (Hobbs and Torreblanca, 2020).

Through the so-called “Brussels effect”, the EU has demonstrated a remarkable capacity to export its regulatory standards, particularly in areas such as privacy and data protection. European regulations such as the GDPR, which governs data privacy, came to be regarded as the “gold standard” of digital regulation on a global scale. The size and attractiveness of the European market meant that, even in the absence of major domestic digital platforms, leading US technology companies operated in Europe under significantly stricter standards than those in force in the US, where the lack of comprehensive federal privacy legislation has resulted in a much looser and more fragmented framework (Bradford, 2020).

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

In an initial phase, the US successfully pressured the EU to decouple technologically from China, particularly in sectors such as 5G networks, thereby depriving Member

States of relevant technological alternatives. Subsequently, Washington began to exploit Europe's dependence on US technology to challenge European regulations and seek exemptions or favourable reinterpretations for its companies. Finally, as Sino-American rivalry has intensified, Washington has stepped up pressure on Brussels to align its regulatory standards with those of the US, describing European regulations as extraterritorial, discriminatory and even extortionate.

This dynamic has placed the EU in a position of structural vulnerability, as it lacks the material capacity necessary to credibly evade coercion from both the US and China. The European strategy of developing indigenous technological alternatives in areas such as semiconductors, cloud computing and artificial intelligence constitutes a rational response, but one that is extremely costly in terms of time, financial resources and political coordination. Consequently, this approach cannot guarantee European digital sovereignty in the short term, forcing the EU to operate for an extended period under conditions of strategic dependence.

US pressure on Europe to reject Chinese technology began during the first Trump administration, but not only continued, it intensified under the Biden administration, particularly through the proliferation of export controls on critical technologies to China. According to the description by then-National Security Advisor Jake Sullivan, the US would build a "small garden with high fences" in the technological sphere (The White House, 2023). However, the inclusion in these restrictions of the three most strategic technologies of the present day—artificial intelligence, semiconductors and quantum computing—showed that this "garden" was far from small. On the contrary, it signalled the launch of a direct challenge to China.

Another revealing episode of Europe's vulnerability vis-à-vis the US occurred with the Dutch government's decision, in direct response to US pressure, to force the company ASML to cease the export of extreme ultraviolet lithography machines, which are indispensable for the manufacture of advanced semiconductors. This case has highlighted the extent to which even Europe's few critical technological advantages could be neutralised by external political decisions (Quin, 2024).

Europe's dependence on private US technology companies has been laid bare even further during the war in Ukraine. In September 2022, Elon Musk ordered a restriction on Ukrainian access to the Starlink low-orbit satellite system, which is crucial for

Ukrainian military communications (Roulette, Bryan-Low and Balmforth, 2025). Musk justified his decision by citing fears of a nuclear escalation. This episode highlighted the risks inherent in essential technological capabilities for collective security being controlled by private actors capable of directly influencing strategic dynamics of the highest order.

The Starlink case marked a turning point for the EU, as it brought into sharp relief the consequences of outsourcing critical infrastructure to foreign private companies. This episode has been compounded by Musk's growing vitriol against the EU during the US election cycle, in line 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 the US commitment to Europe, citing an alleged decline in European democratic standards due to its digital regulations.

Following his appointment as US Vice-President, Vance elevated this criticism to the central tenet of US policy towards 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 described as European "regulatory extortion", in direct reference to legislation on digital services and markets (The White House, 2025a). This explicitly activated the alliance between the White House and major US tech companies, already evident at Trump's inauguration ceremony, which was attended by Silicon Valley's top executives. Figures such as Mark Zuckerberg have equated European regulation with institutionalised systems of censorship comparable, in his view, to those of China. Both Zuckerberg and Musk have openly challenged the Union, refusing to comply with certain obligations relating to the fight against disinformation and online harms on platforms such as X.

Musk's direct interference in European political processes, such as his explicit support for anti-establishment forces like Alternative for Germany (AfD) during the German parliamentary elections in February 2025, has had a significant political impact. Not only for backing an extremist force, but for normalising discourse that trivialised

Germany's historical past, which has been perceived as unprecedented interference by a foreign private actor.

A new source of concern has emerged with the Trump administration's decision to impose sanctions on the International Criminal Court following the issuance of arrest warrants against Israeli Prime Minister Benjamin Netanyahu; the US forced Microsoft to withdraw email services from the prosecutor in charge of the case. The company complied with the order, demonstrating that, under US law, companies must comply first and litigate later, even when this affects international institutions based in Europe (Satariano and Smialek, 2025).

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

Finally, the publication of the US national security doctrine in December 2025 has confirmed Europe's worst fears, by openly legitimising the exploitation of US technological superiority for the purpose of political transformation in Europe. The US strategy describes Europe as a victim of an anti-democratic ideological drift and advocates the need to promote the rise to power of political forces aligned with Trumpism. The fear, from a European perspective, is that the US will replicate—through private digital platforms—tactics of influence like those previously employed by Russia, triggering a head-on transatlantic clash over digital services, regulatory sovereignty and democracy (The White House, 2025b).

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

Building European digital sovereignty

The EU has explicitly recognised that technology constitutes a central dimension of its security and political autonomy (European Commission, 2023). The European

Commission formed following the June 2024 elections gives concrete expression to this recognition by creating, for the first time, an executive vice-presidency dedicated to Technological Sovereignty, marking a turning point in the European conception of power in the 21ST century.

Although the concept of technological sovereignty is not unambiguous—and is particularly complex in a global context characterised by deep interdependencies and cross-cutting vulnerabilities—the European institutions use it to refer to a specific 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 arising from critical dependencies.

From this perspective, ensuring European technological security requires action on three complementary fronts: developing our own capabilities, building resilience against coercion, and defending the democratic space.

The first pillar—unavoidable, yet long-term—consists of developing a European technological and industrial base in those areas where external dependence creates economic or security risks. The mission letter sent by Commission President 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 (European Commission, 2024).

Without its own capabilities in these areas, the EU lacks any real room for manoeuvre. Technological security cannot be sustained solely through regulation if there is no physical infrastructure capable of offering credible alternatives. However, this strategy requires massive investment, coordination between Member States and an explicit political acceptance that industrial policy is an unavoidable necessity for national security.

Given that developing these capabilities will take years, the EU needs short- and medium-term instruments of protection and deterrence 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, makes strategic use of trade policy, bearing in mind that the US maintains a structural surplus with the EU in digital services; second, strengthens competition policy, reducing the market power—and by extension political power—of large technology platforms; thirdly, advance common fiscal instruments, indispensable for financing strategic technological investments and preventing regulatory capture; and fourthly, explore national security tools, including European preference clauses or selective restrictions in sectors deemed critical.

These instruments have already been applied in relation to China, particularly to reduce dependence on Chinese companies subject to legal frameworks that compel them to cooperate with their intelligence services. Given that the US has legislation with comparable extraterritorial effects, the EU must also begin to assess the security risk posed by its exposure to US companies, particularly in areas such as the cloud, digital platforms or data infrastructure.

A third element of European technological security is the defence of 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 with the adoption of the so-called “democratic shield”, which explicitly recognises electoral processes as critical infrastructure on a par with energy or transport infrastructure

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

Despite its vulnerability in other areas, the EU has demonstrated that it must not relinquish its regulatory power. The effective application of European digital legislation to large tech companies, including penalties for non-compliance, constitutes one of the few instruments of structural power at the EU’s disposal. Giving ground in this area would not reduce external pressure, but rather increase it, by confirming that technological dependence can translate into political subordination. Regulatory firmness is not incompatible with transatlantic cooperation; indeed, it is a prerequisite for such cooperation to be based on more symmetrical relations (Torreblanca, 2025).

In a world where there are only two major technological poles—the US and China—the EU faces the risk of becoming a digital colony if it does not act decisively. Paradoxically, its vulnerability is currently greater vis-à-vis the United States than vis-à-vis China, precisely because of the depth of existing interdependence. Ensuring European technological security therefore requires a combination of ambitious industrial policy, instruments of defence against coercion, protection of the democratic space and sustained political will. Technological sovereignty is not an end in itself, but a necessary condition for preserving the European political, economic and social model in an increasingly competitive and coercive international environment.

Conclusion

Technology has become a central factor in international power, comparable to territory, population or strategic resources. The current technological revolution, characterised by its speed, global reach and the structural role of private actors, is accelerating the securitisation of innovation and pushing the international system towards a logic of rivalry, fragmentation and competition between technological blocs led by the US 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 its lack of its own industrial capabilities in critical technologies exposes it to dependencies that already translate today into extreme vulnerability to external coercion.

Regulation alone is not enough to defend European sovereignty in an increasingly hostile geopolitical environment. Ensuring European technological security therefore requires an integrated strategy that combines long-term industrial policy, instruments of resilience and deterrence against technological coercion, and enhanced protection of the democratic sphere 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 21ST century.

Bibliography

Alandete, D. (2017). The Russian plot used Chavista networks to gain influence in Catalonia [online]. *El País*. [Accessed: 15 January 2026]. Available at: https://elpais.com/politica/2017/11/10/actualidad/1510341089_316043.html

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

BBC News. (2020). Huawei ban: UK to impose early end to use of new 5G kit [online]. BBC News. [Accessed: 15 January 2026]. Available at: https://www.bbc.com/news/business-55124236

Biden, J. (2025). President Biden's Farewell Address. The White House, 15 January [online]. The White House. [Accessed: 15 January 2026]. Available at: https://www.presidency.ucsb.edu/documents/farewell-address-the-nation-4

Bria, F. (2025). The coup d'état by the techno-authoritarians: from post-democratic America to the Europe to come [online]. *La Vanguardia*. [Accessed: 15 January 2026]. Available at: https://www.lavanguardia.com/internacional/20251102/11220880/golpe-tecnoautoritarios-america-postdemocratica-europa-viene.html

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

—. (2023). *Digital Empires: The Battle for Global Tech Dominance*. New York, Oxford University Press.

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

European Commission. (2023). Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy" (JOIN/2023/20 final) [online]. European Commission. [Accessed: 15 January 2026]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0020

—. (2024). Mission Letter from Ursula von der Leyen, President of the European Commission, to Henna Virkkunen, Executive Vice-President-designate for

Technological Sovereignty, Security and Democracy [online]. European Commission. [Accessed: 15 January 2026]. Available at: https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf

Feldstein, S. (2019). *The Global Expansion of AI Surveillance* [online]. CEIP. [Accessed: 15 January 2026]. Available at: https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

Fernández, J. J. (2024). The army identifies a Russian influence network in Spain comprising 179 spokespersons. *El Periódico*. [Accessed: 15 January 2026]. Available at: https://www.elperiodico.com/es/politica/20240718/ejercito-ecosistema-desinformacion-ruso-espana-altavoces-105779287

Ferracane, M. F., Marel, Erik van der and Lee-Makiyama, H. (2018). *Digital Trade Restrictiveness Index* [online]. Brussels, European Centre for International Political Economy (ECIPE). [Accessed: 15 January 2026]. Available at: https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

Financial Times. (2022). US hits China with sweeping tech export controls [online]. *Financial Times*. [Accessed: 15 January 2026]. Available at: https://www.ft.com/content/6825bee4-52a7-4c86-b1aa-31c100708c3e

Headrick, D. R. (1979). *The Instruments of Empire: Technology and European Colonialism in the NINETEENTH Century*. Madrid, Alianza**.**

Hobbs, C., Puddephat, A. and Torreblanca J. I. (2016). The Geoeconomics of the Digital. In: Leonard, M. (ed.). *Connectivity Wars: Why Migration, Finance and Trade and the Geo-Economic Battlegrounds of the Future* [online]. European Council on Foreign Relations. [Accessed: 15 January 2026]. Available at: https://ecfr.eu/archive/page/-/Connectivity_Wars.pdf

Hobbs, C. and Torreblanca, J. I. (2020). *Europe's Digital Sovereignty*. Madrid, Catarata.

Hu, K. (2023). ChatGPT sets record for fastest-growing user base in history [online]. *Reuters*. [Accessed 15 January 2026]. Available at:

https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/

Kissinger, H. A., Schmidt, E. and Huttenlocher, D. (2021). *The Age of AI: And Our Human Future*. Little, Brown and Company.

Leonard, M. (2021). *The Age of Unpeace: How Connectivity Causes Conflict*. Bantam Press.

Qin, S. (2024). ASML Cancels Some Shipments to China at Biden Administration's Request [online]. *The Wall Street Journal*. [Accessed: 15 January 2026]. Available at: https://www.wsj.com/tech/netherlands-blocks-asml-exports-of-some-chip-making-equipment-to-china-2fe4a162

Roulette, J., Bryan-Low, C. and Balmforth, T. (2025). Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia [online]. *Reuters*. [Accessed: 15 January 2026]. Available at: https://www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/

Sánchez, I. and Torreblanca, J. I. (2023). Ukraine one year on: When tech companies go to war [online]. European Council on Foreign Relations. [Accessed: 15 January 2026]. Available at: https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/

Satariano, A. and Smialek, J. (2025). Europe's Growing Fear: How Trump Might Use U.S. Tech Companies Against Europe [online]. *New York Times*. [Accessed: 15 January 2026]. Available at: https://www.nytimes.com/2025/06/20/technology/us-tech-europe-microsoft-trump-icc.html

Schwirtz, M. and Bautista, J. (2021). Married Kremlin Spies, a Shadowy Mission to Moscow and Catalonia [online]. *New York Times*. [Accessed: 15 January 2026]. Available at: https://www.nytimes.com/2021/09/03/world/europe/spain-catalonia-russia.html

Taylor, J, Ewing, P. and Johnson, C. (2018). Grand Jury Indicts Russians Linked To Interference In 2016 Election [online]. *National Public Radio*. [Accessed: 15

January 2026]. Available at: https://www.npr.org/2018/02/16/586500591/grand-jury-indicts-russians-linked-to-interference-in-2016-election

Torreblanca, J. I. (2020). Democracy and social media. In: Lapuente, V. and Costas, E. (eds.). *How to save liberal democracies* [online]. Madrid, Círculo de Empresarios, pp. 131–150. [Accessed: 15 January 2026]. Available at: https://circulodeempresarios.org/app/uploads/2020/06/Libro-Democracias-Liberales-OK-paginas.pdf

—. (2021). Technology. In: Leonard, M. and Krastev, I. (eds.). *The Power Atlas: Seven Battlegrounds of a network world* [online]. European Council on Foreign Relations. [Accessed 15 January 2026]. Available at: https://ecfr.eu/wp-content/uploads/power-atlas.pdf

—. (2025). Big tech, Donald Trump, and techno-imperialism: How Europe can avoid becoming a digital colony [online]. European Council on Foreign Relations. [Accessed: 15 January 2026]. Available at: https://ecfr.eu/article/big-tech-donald-trump-and-techno-imperialism-how-can-europe-avoid-becoming-a-digital-colony

Vance, J. D. (2025). Speech by J.D. Vance. J.D. Vance (Vice President, United States of America) speaking on "The U.S. in the World" [online]. Munich Security Conference. [Accessed: 15 January 2026]. Available at: https://securityconference.org/en/medialibrary/asset/the-speech-of-jd-vance-20250214-1817/

Washington Post. (2017). Catalonia held a referendum. Russia won. 2 October 2017. Available at: https://www.washingtonpost.com/opinions/global-opinions/catalonia-held-a-referendum-russia-won/2017/10/02/f618cd7c-a798-11e7-92d1-58c702d2d975_story.html

The White House. (2023). Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution [online]. The White House. [Accessed: 15 January 2026]. Available at: https://www.presidency.ucsb.edu/documents/remarks-national-security-advisor-jake-sullivan-renewing-american-economic-leadership-the

—. (2025a). Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties [online]. The White House. [Accessed: 15 January 2026]. Available at: https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/

—. (2025b). *National Security Strategy of the United States of America* [online]. Washington, DC, The White House. [Accessed: 15 January 2026]. Available at: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

*José Ignacio Torreblanca**

Professor of Political Science and Public Administration at the UNED and Distinguished Policy Fellow, Geoeconomics and Technology Programme, European Council on Foreign Relations