BRIEFING

European Parliament

The geopolitics of technology

Charting the EU's path in a competitive world

SUMMARY

The emergence of a contested multipolar world, one that is increasingly inward looking and unstable, has been paralleled by profound technological change and deepening digitalisation of economies and societies. Technology has become a battleground in the geopolitical quest for power. Global technological rivalries – broadly divided between countries promoting liberal and human-centric governance models and those deploying technology to support authoritarianism – are reshaping the world. Other undecided countries are meanwhile sitting on the fence.

A case in point is the intensifying Sino-American tech rivalry, including in the pivotal artificial intelligence (AI) and semiconductors sectors. In addition to its deep impact on economies and competitiveness, technology is also at the core of geopolitical struggles through its deployment in cyberwarfare, election interference and misinformation.

Supporting open trade, a multilateral order and global standards have always been among the EU's fundamental principles. To safeguard those values and navigate this new, challenging, fractured and confrontational environment, the EU has been developing a policy toolkit for quite some time. Additionally, it has frequently been a front-runner in regulating critical emerging technologies, while also establishing partnerships with allies and like-minded countries, safeguarding its internal market and addressing technological vulnerabilities and strategic dependencies.

Since the underlying trends are unlikely to weaken, the issues at the nexus of geopolitics and technology are expected to feature prominently on the European Parliament's agenda during its 2024-2029 legislature. Experts recommend that to maintain its normative heft, the EU needs to build its industrial prowess by boosting its technological capacity, investing in digital infrastructure and financing innovation. The EU should also strengthen ties with like-minded countries and engage the Global South, expand its economic security policy and enhance the Global Gateway initiative. Boosting competitiveness and striking the right balance between autonomy and openness as well as between security and free trade, remain the key challenges in a world shaped by multiple crises and disruptive technologies.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

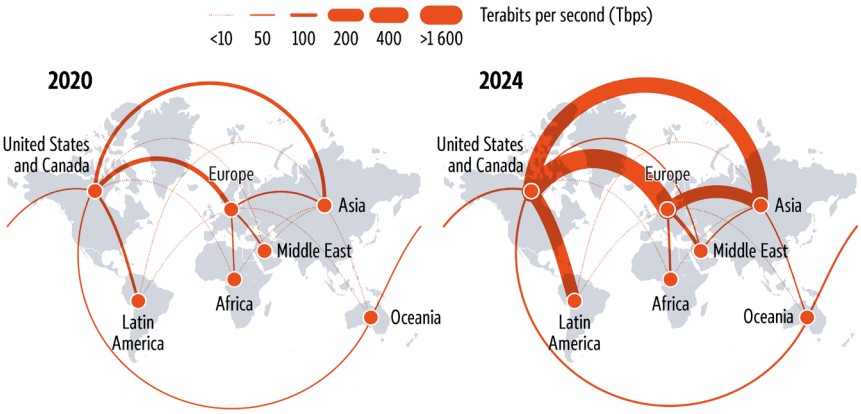
Author: Marcin Szczepański; Graphics: Eulalia Claros and Samy Chahri
Members' Research Service

PE 762.384 – September 2024

EN

Context

Figure 1 – International data traffic in 2020 and 2024



Data source: UNCTAD, 2021.

The 2008 global financial and economic crisis marked the end of a decades-long era of progressive globalisation. The ensuing 'slowbalisation' is characterised by weakened trade flows, a prolonged slowdown or reversal of global trade liberalisation, the emergence of trade barriers, weakening political support for open trade, a crisis of multilateralism, and intensifying geopolitical tensions. Until recently, the focus was on facilitating the mobility of physical goods by lowering transport costs and protectionist barriers, while now it is on reducing barriers to the flow of information, technology and ideas. Globalisation has slowed down in a world that is more inward looking, tense and assertive, as well as being marked by growing ideological differences. At the same time, the digitalisation of the economy and society has surged (see Figure 1), not least due to the pandemic. According to Goldman Sachs, the present era of significant technological developments is also the most geopolitically unstable one since the Cold War, as manifested by the 'intensifying competition between the US and China, wars in Europe and the Middle East, and shifting global alliances'. Rising geopolitical risks are a sign that the established post-war global order based on the dominance of the West is under pressure to make way for a new multipolar world characterised by fragmentation and instability. In the technological sphere, this is evident in the competing visions for a global digital order, varying norms and divergent standards and protocols.

The nexus between technological innovation and the quest for global domination has a long history, dating back centuries. However, in recent times, new technologies such as 5G, artificial intelligence (AI), nanotechnology and robotics have become more intertwined than ever with geopolitical, economic and trade interests. According to Chatham House, world powers are using these new technologies 'to exert power and influence and to shape geopolitics'. High-tech weapons systems enhance military prowess, while new platforms and the standards that govern them increase economic leverage. Additionally, cutting-edge research and innovation amplify global impact.

Mark Leonard from the European Council on Foreign Relations suggests that there is now 'a new map of power in the modern world that is no longer defined by geography, by control of territory or oceans but rather by control over flows of people, goods, money and data and by exploiting the connections technology creates'. As a result, virtually every connection between countries – from energy flows to IT standards – has become a tool of geopolitics. While this tool is neither inherently good nor bad, political players deploy it with specific motives and incentives in mind. Furthermore, geopolitical risks and technology are highly integrated into political developments, and geopolitical conflicts are spurring technological development. Current technology is considered to already constitute a strategic battleground for future geopolitics. Nowhere else is this manifested more clearly than in the epoch-defining competition between the US and China, called 'the biggest geopolitical test of the 21st century' by US Secretary of State Antony Blinken. This is essentially an increasingly heated technological competition between the two political rivals, both seeking to establish, defend or widen their geographical and sectoral spheres of influence by controlling innovative technologies.

Technology and global rivalries

The increasing tendency of countries to look inward also affects the sphere of technology. Countries are imposing trade controls through regulations, export controls, entities lists, and localisation requirements to secure access to critical technologies for themselves. A case in point is the geopolitical competition shaping the world in relation to semiconductors and critical raw materials. Cyberspace, which has no territorial boundaries, is increasingly becoming an arena of rivalry and conflict. When it comes to the EU, security risks, the role of global tech giants and global norms that do not align with its interests are some of the major challenges facing it.

The Observer Research Foundation (ORF) maintains that the evolution of ever-expanding digital technologies, along with their high level of influence without corresponding accountability, has redefined the concept of digital sovereignty. The EU considers digital sovereignty to be the ability to act independently in the digital world. The ORF sees two distinctive, competing models of tech governance and digital sovereignty in existence: a libertarian/democratic one followed in the West, and an intrusive, authoritarian one practiced in countries like China. According to Freedom House, China had the world's worst environment for internet freedom in 2023 for the ninth consecutive time.[1] For the former camp, control of technology is mostly about competitiveness, economic supremacy and security. For the latter, it is also about control of citizens, misinformation and propaganda, interference in democratic processes and surveillance both domestically and abroad.

China: Geopolitics in motion

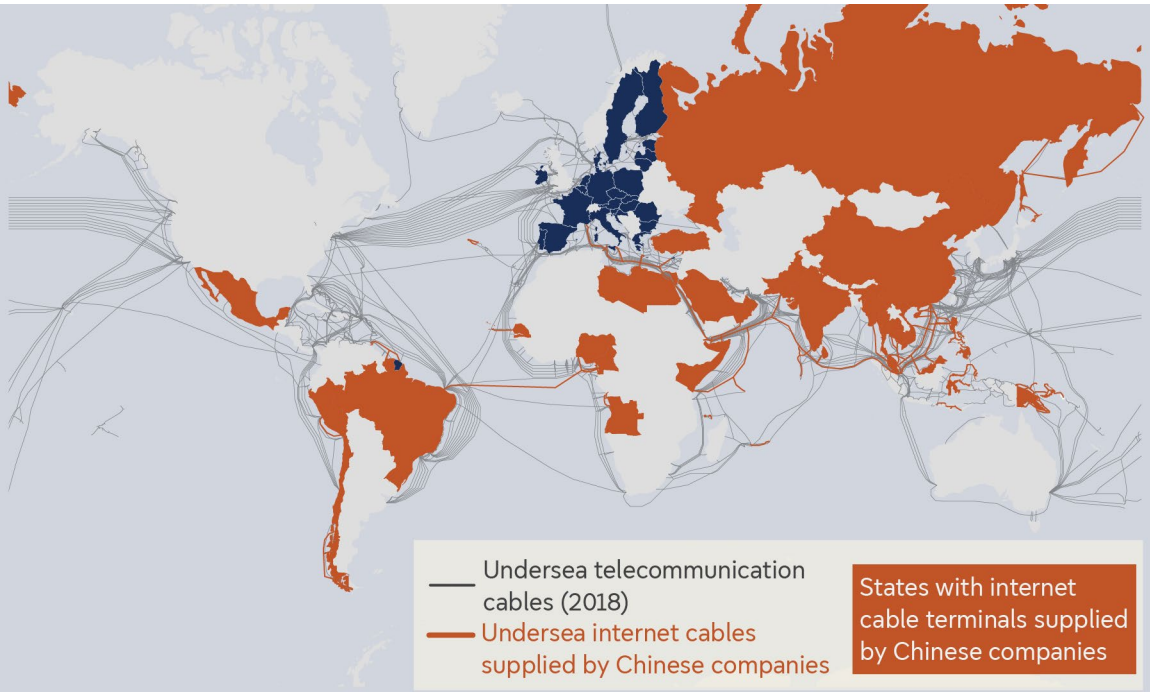
In 2015, the Chinese Communist Party launched its 'Made in China 2025' strategy, with the goal of transforming the country into a self-sufficient global high-tech powerhouse by 2049. During the pandemic, China developed its corollary, the dual circulation model, as a response to the new geopolitical realities. This model aimed to reduce the country's reliance on external inputs and partners by fostering domestic innovation and self-sufficiency. Through public-private partnerships, direct subsidies to the private sector and support for state-backed companies in recent years, China has allocated massive funds to achieve its goal of coming out first in the race for technological dominance. At present, while the US remains a dominant player in the development of most breakthrough technologies and in the innovation, commercialisation and scaling of emerging and existing technologies, the gap between the two countries is narrowing.[2]

China's growing international ambitions are evident in its Belt and Road Initiative (BRI) and – in the technological sphere – its offspring, the Digital Silk Road (DSR). The BRI draws countries into Beijing's orbit by offering them financing for infrastructure development and creating economic interdependencies, while the DSR adds the digital component to further China's ambition of securing a dominant position in the technological sector. Estimates indicate that at least a third of the 150+ countries cooperating with China under the BRI may also be involved in the DSR. Experts note that: 'the DSR goes beyond the technology infrastructure, which raises two critical concerns by giving China leverage to advance the digital authoritarian governance model and jeopardizing data privacy'. The Council on Foreign Relations highlights the fact that recipients of the DSR may have (and some already have) requested China to develop surveillance capabilities and ways to control and censor the internet. These 'digital repression' countries are also themselves at a heightened risk of espionage and coercion.

The European Council on Foreign Relations argues that China also 'uses digital disinformation to influence public opinion in other countries, mounts cyberattacks and cyberespionage to strengthen its industrial base, and strategically deploys attractively-priced 5G technologies abroad to gain control of telecom networks'. There are widespread accusations that in the battle for technological supremacy, China pursues unfair economic policies, such as systemic infringement of intellectual property rights, forced technology transfers and engagement in cyber-theft and industrial and academic espionage.

Many experts believe that China uses digital infrastructure, such as submarine cables, to exert geopolitical influence. The US has largely prevented China from putting in place a global undersea cable infrastructure due to concerns about espionage and potential disruptions in the event of a conflict. Nonetheless, China has still managed to make inroads by creating networks spanning five continents and many countries (see Figure 2).[3] This has increased the risks of internet fragmentation, potentially leading to a more centralised, tightly controlled and surveilled system. Internet restrictions already exist in countries such as China, Russia, Saudi Arabia, Iran and Pakistan.

Figure 2 – Undersea internet cables supplied by China



Data source: TeleGeography, 2024.

Standards are yet another indispensable tool for advancing geopolitical goals through technology. A relative latecomer to international standardisation, China is now increasingly eager to influence international standards for emerging technologies. To this end, it has stepped up its participation in key bodies, such as the International Telecommunication Union (ITU), the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and in bilateral cooperation frameworks. It has also expanded the BRI and DSR and drawn up its China Standards 2035 strategy focused on the development of technology standards and their internationalisation. China is engaged in creating new standardisation research institutes, certification centres and standards innovation bases, and in handing out subsidies to researchers and companies for standards-related work.

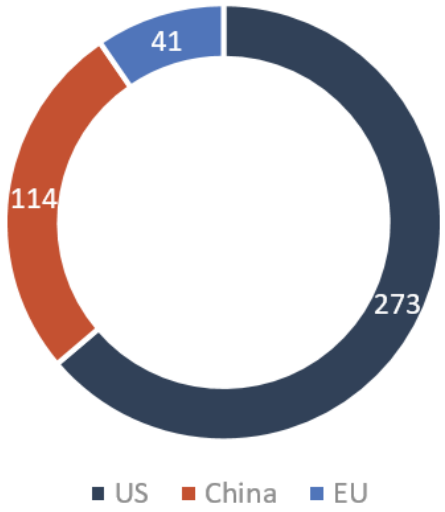
Sectoral view: AI and semiconductors

AI has the potential to revolutionise multiple sectors of the economy and spheres of life. The Brookings Institution famously stated that 'Whoever leads in artificial intelligence in 2030 will rule the world until 2100.' While AI has a myriad of possible geopolitical impacts, some major ones are as follows. The leaders in AI will not only benefit from enormous economic gains and enhanced military capability but will also set norms, standards and technology trends for the rest of the world. Researchers also see that AI has the potential to exacerbate divides both within and between countries, due to the unequal distribution of related benefits and knowhow.AI is also likely to redefine global supply chains and revolutionise warfare. Furthermore, it may change the balance of power between states, as their responses to challenges posed by AI and their ability to reap benefits

from it are likely to play a key role in their international standing.[4] AI's critical nature has made it the frontier of global geopolitical competition, especially between the US and China. Most observers agree that the US remains the global leader in AI (also due to the rise in generative AI), but that the distance dividing it from China is narrowing. A 2022 Joint Research Centre report ranks the EU third in economic terms, but argues that its distance from the US and China is shorter than often suggested. However, while the EU is strong in regulating AI, this is not supported by funding, particularly from the private sector (see Figure 3).

Closely connected to AI, **semiconductors** are the key building block of the modern technological and information economy. Semiconductors are the backbone of a myriad of key industries, ranging from automobiles to aerospace and defence. They are the 'new driver of geopolitical balance', as they power critical emerging technologies such as AI, 5G, quantum computing and industrial automation. No single country can achieve self-sufficiency or supremacy in all aspects of semiconductor production. The value chains are global and complex, and just a few countries hold dominance in their segments: the US for chip design, Japan for materials, and Taiwan for manufacturing. The EU semiconductor industry is well positioned to cater to the automotive, aerospace and industrial automation sectors. Furthermore, the EU is ahead in terms of sustainability, this being a long-term growth driver, and EU companies are global leaders in producing chip manufacturing equipment and its associated supply chain.

Figure 3 – Total venture capital investment in AI in 2020-2023 (US$ m)



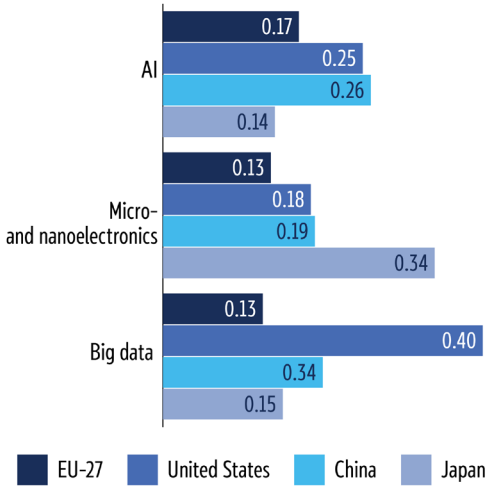
Data source: OECD, 2024.

As the main semiconductor hubs are in Taiwan, China and South Korea, value chains are particularly vulnerable to geopolitical tensions. The stakes and risks are high, as antagonisms between major players like the US and China can escalate and trigger broader economic conflict with potentially disastrous effects across many semiconductor-dependent sectors. Patents, copyrights and intellectual property protection are all crucial to chip innovation and competitiveness, which amplifies concerns about espionage, cyber theft and unauthorised technology transfer. National security adds another layer of complexity to semiconductor geopolitics. As chips are now essential components in defence systems, telecommunications infrastructure and other critical sectors, they may serve as the reason for potential restrictive sectoral measures.

In the high-tech sector, including AI and semiconductors, navigating the intensifying Sino-American rivalry remains a key issue for the EU. This rivalry began during the Obama administration, gained momentum during Trump's and has further escalated during Joe Biden's. Since the EU relies on global standards and markets, the fragmentation and divergence of global tech resulting from this rivalry are not serving its interests well. The EU's lack of leadership in key technological areas further complicates its position. According to the Commission's report on strategic dependencies, the EU is performing less well than the US and China in both AI and micro-and nanoelectronics (which include semiconductors), and in big data (which underpins both of these sectors). This assessment takes into account a composite index of new technologies generation, start-up creation and skills (see Figure 4). In the AI domain, the EU is working with the US on a common vision and standards, while many of its companies cooperate with China on research. Regarding semiconductors, the EU collaborates with the US on monitoring global supply chains and state aid levels, and is integrated with both China and the US in complex supply chains. The EU is dependent on China for essential raw materials and to a lesser extent for packaging, assembly and testing, and chip fabrication. The EU's deep economic ties with both adversaries are yet another complicating factor.

The complexity and vulnerability of the EU's position is well illustrated by the recent US export controls, introduced in October 2022 by the Biden administration to make it harder for China to access or produce advanced computer chips and to obtain relevant technology, manufacturing equipment and know-how. The goal is to slow down Beijing's progress in AI and make it very hard for it to develop supercomputers with military applications. These controls ban US companies from exporting critical chip manufacturing and prevent US citizens and companies from providing direct or indirect support to Chinese companies involved in advanced chip manufacturing. Additionally, the US has placed a number of companies on the Entity List, a blacklist banning these companies from exporting certain technologies. These restrictions were further tightened in October 2023, with Washington reportedly considering even more restrictive actions. These controls are essentially of an extraterritorial nature and reflect a growing trend in US export control laws over in recent years.

Figure 4 – Global leaders' performance in selected key technologies



Data source: European Commission, 2021.

In response, China initiated a WTO dispute in December 2022, increased investment in its domestic sector, and imposed export restrictions on germanium and gallium, both critical to chip manufacturing. To prevent circumvention of the measures, the US successfully lobbied and negotiated with the Netherlands (where ASML, the leading manufacturer of equipment for advanced chips, is located) and Japan to implement similar controls. Reportedly, this unilateral imposition of export controls by the US was considered strong-arm tactics by its allies. Dutch lawmakers questioned their country's participation in the second round of controls, with the trade minister emphasising the importance of negotiating these controls in coordination with other EU Member States.[5] Reportedly, ASML, which has already pulled some of its staff out of China, has now been asked to stop servicing machines already installed there.

Such situations pose multiple risks to the EU and its companies. Experts recognise that the EU is vulnerable when it comes to defending itself against extraterritorial measures. In contrast, the US has a robust system and could impose export controls on EU companies in the chip supply chain that rely on US intellectual property if they do not comply. US sanctions may also compel China to focus on less sophisticated chips, leading to oversupply and potentially driving EU chip suppliers out of the market. Other companies may replace the EU companies, depriving them of revenue. On the other hand, if the EU complies with US controls, China may retaliate in other sectors and do so in an unpredicted or a seemingly unlinked manner, leveraging its position as a major supplier of over half of all products used in the EU's most sensitive industrial ecosystems. The European Think-tank Network on China has summarised the EU's geopolitical stand, saying that it strives to 'develop a distinct political positioning in a context of polarized international relations...without being necessarily forced to take sides'.

Technology, democracy and security

In recent years, the authoritarian wave sweeping the world has led to a decline in the level of democracy enjoyed by the average person, comparable to levels seen in the mid-1980s. More than 70 % of the world's population now resides in countries that are becoming increasingly authoritative. About half of the nearly 1 000 experts surveyed by the Pew Research Center predicted that the use of technology will weaken core aspects of democracy and democratic representation between 2020

and 2030. This is mostly due to the expansion of digital technologies and social media, as well as the alteration of the information landscape, where high-quality information is available to those who can afford to pay for subscriptions, while the vast majority relies on free content of questionable quality, leading to the division of societies into information bubbles. Once trapped in bubbles of content that matches their own views, users lack access to alternative perspectives, reinforcing their misconceptions and pushing them towards more extreme content. The Lowy Institute has assessed that 'decentralisation and rapid increase of information and content production... made the public sphere more cacophonous, limiting the ability of citizens to engage in productive dialogue'.

While modern communication channels can be used in authoritarian states to challenge the regime, experts agree that modern technologies have led to declining political trust, increasing populism and growing polarisation in established democracies. New tech platforms are believed to heighten the effectiveness of misinformation and disinformation, as well as promote non-consensual and confrontational debates. There are also serious geopolitical concerns related to AI: used in many countries as a tool of oppression and surveillance, it is also being increasingly deployed to influence elections through novel methods such as deepfakes. Information space, which is highly dependent on technology, is where the battle over foreign information manipulation and interference (FIMI) takes place. This was identified in the Strategic Compass – a plan of action for the EU's security and defence until 2030 – as a rapidly growing risk to international security and stability, but also to the EU and its immediate neighbourhood. While Russia and China are prominent FIMI players, many other countries also deploy technologies for malicious purposes. An Oxford University study identified over 80 countries using social media to spread computational propaganda and disinformation.

Russia's involvement in the UK's referendum on EU membership

The UK Parliament's Intelligence and Security Committee conducted an investigation into the Kremlin's influence in UK politics and published its findings in a 2020 report. The report stated that 'Russian influence in the UK is the new normal ... the UK is clearly a target for Russian disinformation'. It did not try to assess the impact of Russian involvement on the outcome of the vote, as that would be difficult, if not impossible. However, it noted that social media companies, 'which hold the key', are 'failing to play their part' and urged the government to take action to compel these companies to 'take covert hostile-state use of their platforms seriously.'

Experts found that Russia was using social media and bots to amplify anti-EU sentiments and pro-Brexit messages by producing fake or inflammatory stories. Russian hackers also attempted to carry out cyberattacks on the UK energy, telecommunications and media industries.

Another geopolitically important arena of confrontation between democracy and authoritarianism is cyberwarfare. A 2024 study by the EU Agency for Cybersecurity, ENISA, concluded that the hardening geopolitical situation accelerates the need for stronger cyber crisis management in the EU. ENISA also reported a significant increase in both the variety and quantity of cyberattacks and their consequences since the start of the war in Ukraine. The EU has been exposed to malicious practices such as those causing damage to critical infrastructure (including digital infrastructure), ransomware attacks, malware, social engineering, threats against data and service availability and supply chain attacks. In this aspect, it is crucial to protect critical infrastructure – ranging from undersea cables to data centres – not only from cyberattacks but also from politically motivated investment that is undesirable.

EU actions

In 2019, Commission President von der Leyen shared her vision of a Geopolitical Commission with the European Parliament. Not long afterwards, the war in Ukraine accelerated and magnified existing geopolitical trends and challenges, putting technology even more into the spotlight.

The EU has been attempting to influence global standards by leveraging the appeal and power of its internal market and by aiming to establish the Brussels effect in the technological domain as well.

An early example of this is the General Data Protection Regulation, which has had a lasting impact and influenced data practices worldwide. The acts on digital services and the digital markets, along with the EU regulations on artificial intelligence and data governance, have the potential to create similar global effects. The EU's aspiration to take the lead in global standard setting is clearly reflected in its 2022 standardisation strategy.

The EU also seeks to establish digital partnerships with like-minded countries and partners from the Global South in order to offer an alternative to the Chinese DSR. The main vehicle here is the Global Gateway, which finances projects (including infrastructure) that enable the digital transition in line with EU values and standards.[6] The Commission has launched a number of initiatives at the nexus of geopolitics and technology: the Trade and Technology Council with the US (see box) and India, as well as digital partnerships with Canada, Japan, Singapore and South Korea, which complement free trade agreements with these countries that have dedicated digital chapters.[7]

The EU is also working closely with partners and allies to establish and promote common positions on technological issues in international and multilateral bodies such as the standardisation organisations, the WTO and the G7. Some joint initiatives of the EU and its partners and allies, such as the Declaration for the Future of Internet, the UN General Assembly resolution on AI, and the OECD Global Partnership on Artificial Intelligence, are considered to have significant potential to shape democratic technological standards globally. Furthermore, EU-US Trade and Technology Council is a high-level transatlantic cooperation forum that covers indispensable topics such as investment screening, export controls (fundamental to sanctions against Russia), security of supply chains, convergence in regulating emerging technologies, standard setting (e.g. in AI), coordination of positions in relevant international bodies, disinformation and FIMI.

EU economic security

In June 2023, the Commission adopted a communication to strengthen the EU's economic security during a time of growing geopolitical tensions and profound technological shifts. It launched assessments of the EU's risks related to the resilience of supply chains, physical and cyber security of critical infrastructure, technology security and technology leakage, weaponisation of economic dependencies and economic coercion.

This was followed by a package in January 2024, consisting of: (i) the revision of the FDI screening framework; (ii) ways to improve the export controls regime; (iii) deliberations on risks from outbound investment in critical technologies such as semiconductors, AI, quantum technologies and biotechnologies; (iv) measures to enhance research security to prevent undesirable transfers of critical technology, malign influence, and ethical or integrity violations by third countries; and (v) options for boosting support for research and development of dual-use technologies.

The Commission underlined that the implementation of the economic security strategy is an ongoing process, and further initiatives will be proposed in due time. The political guidelines for the 2024-2029 Commission put advancing economic security and economic statecraft high on the priority list.

In recent years, the EU has also increased its efforts to safeguard its internal market and address the technological vulnerabilities laid bare during times of pandemic and war. After some high-profile cases of EU companies being taken over by external entities, such as the case involving the acquisition of German robotics leader KUKA by Chinese company Midea, the EU has implemented a foreign direct investment screening framework to prevent undesired takeovers of critical technology. Since many cutting-edge technologies can have military applications as well, the EU has updated its export control rules to prevent their uncontrolled dissemination. Furthermore, to protect itself from interference and unfair market practices in times of intense geopolitical competition and a weakening multilateral order, the EU has adopted one regulation on enforcement and another on foreign subsidies, and an anti -coercion instrument.

To boost its strategic value chains, the EU has started creating industrial ecosystems in critical technologies such as batteries and semiconductors (Chips Act). It also supports innovation and research in emerging technologies, such as AI and quantum computing, through programmes such

as Digital Europe and Horizon Europe. A dedicated hub supports Innovation in defence. Recognising the importance of critical raw materials (CRMs) for technologies, the EU has intensified its efforts in this area as well, by adopting the CRMs Act, conducting trade negotiations through dedicated partnerships and boosting its domestic mining capacity, among others.[8] To facilitate the uptake and the scaling up of strategic technologies' development and manufacturing, the EU has established a strategic technologies for Europe platform (STEP) encompassing digital and deep technologies, clean technologies, biotechnologies and their respective value chains, as well as related CRMs.

To address cybersecurity risks, the EU has developed a cybersecurity strategy, adopted the Cybersecurity Act, the second Network and Information Security Directive, and is finalising the Cyber Resilience Act. It is also developing ways to cope with hybrid threats and foreign influence operations within the EU, and has established structures for greater cybersecurity cooperation and rapid response teams to collectively respond to cyber incidents. Additionally, the EU has been actively addressing FIMI through initiatives such as The East StratCom Task Force (ESTF), EUvsDisinfo, the action plan against disinformation, the anti-disinformation hubs and a defence of democracy package. It is also worth mentioning that the Digital Services Act obligates platforms to be active on mitigating risks such as disinformation or election manipulation. Likewise, the landmark AI Act addresses misinformation and deep fakes in the technology field.

European Parliament

In its resolution of 16 September 2021 on a new EU-China strategy, Parliament underlined that the future strategy on relations with Beijing should provide the necessary tools and data to address the political, economic, social and technological threats stemming from China, as well as the implications for the EU's open strategic autonomy and the multilateral rules-based order. It also called for the development of global standards for the new generation of technologies in line with democratic values and in partnership with like-minded entities.

In its resolution of 9 March 2022 on foreign interference, Parliament stressed that the EU's lack of investment in technology has contributed to its current dependence on foreign suppliers. Parliament believes that the Chips Act represents an important step in reducing dependence on third countries such as China and the United States. In its resolution of 28 February 2024 on common foreign and security policy, Parliament called for stronger transatlantic cooperation on trade and on combating the challenges posed by rapid technological changes and growing cyber threats. It also stressed

Possible issues for the new Parliament

The expert community identifies a number of issues that will need to be discussed in the 2024- 2029 legislative term. Institut Montaigne argues that the use of **extraterritoriality** is increasing exponentially in a world dominated by fractured politics and tech rivalry. However, this issue remains a blind spot in the EU's economic security strategy. The think-tank calls on the new Parliament and Commission to reflect on the challenges and opportunities that extraterritoriality presents for the EU.

The Atlantic Council predicts a heated debate on the **potential outbound investment screening mechanism**, and more specifically on the related issues of national and EU-level competence and possible scope. The Atlantic Council expects that the mechanism will primarily address technology security and technology leakage, and be non-discriminatory towards specific countries.

The Clingendael Institute sees the need for a **new export control regime**, as modern technologies are developing at an unprecedented pace and are often beyond the government's oversight. This situation renders the current system, originally designed for goods transitioning from military to civilian use, inadequate, as this direction has reversed.

Parliament will also play a role in shaping the **revised FDI screening framework**, and Concurrences expects a debate on the balance that needs to be struck between the mechanism's effectiveness and the attractiveness of investment in the EU. Additionally, it notes that legislators face 'an uphill path' due to national security being a Member State competence.

The European Policy Centre advocates for a **new industrial policy and financing framework** to maintain EU competitiveness in AI. Implementing the AI act will likely involve **sector-specific complementary legislation**.

the need for multilateral solutions to new technological challenges and realities, including cybersecurity, biotechnology and AI.

Parliament's resolution of 3 May 2022 on AI in the digital age called on the Commission only to propose legislative acts in the form of regulations for new digital laws in frontier technologies, such as AI, to facilitate the genuine harmonisation of the digital single market. It also highlighted that due to rapid technological advancements, digital legislation should always be flexible, principle-based, technology-neutral, future-proof and proportionate, while adopting a risk-based approach.

In its resolution of 23 November 2023 on the Strategic Compass and EU space-based defence capabilities, Parliament called for the EU to adopt a genuine industrial policy and support investment in key technologies to reduce strategic dependence on third countries, including through joint procurement of critical components and by securing the critical raw materials supply chains.

In their resolution of 14 December 2023 on increasing innovation, industrial and technological competitiveness, Members stressed the need to boost investment and advancements in digital infrastructure to keep pace with evolving technologies and remain at the forefront of innovation on the global stage. They also highlighted the importance of cultivating a technology landscape that fosters both competition and innovation. Additionally, they pointed out that regulatory mechanisms must adapt and evolve in sync with technological advancements and market shifts to uphold the EU's competitiveness and innovation.

Expert views

A recent study conducted by the French Institute of International Relations examined the technology policies of middle powers and their relations with the three main global poles of power: the EU, the US and China. [9] It concluded that the EU primarily projects its influence through the setting of new norms, while the US does this through the strength of its digital services, private sector investment and robust bilateral security ties. As for China, its increasing influence is reinforced by major infrastructure projects and investment abroad. All middle powers are working to balance their relations with these three leaders, and with the exception of Russia, none have clearly 'picked a side' and severed ties with others.

The Massachusetts Institute of Technology Center for International Studies argues that, contrary to much commentary, the US-China strategic competition is not a 'new cold war' because the world is not divided into two adversarial ideological camps aligned with Beijing or Washington. Dealing with China primarily requires revitalising and stimulating economic and technological competitiveness and providing tangible alternatives to the BRI for countries targeted by Beijing for influence.

The Economist warns that the biggest negative effect of the intensifying tech wars could be the division of the world's information and energy-technology industries, resulting in weakened economic growth and slower decarbonisation. These wars are also likely to accelerate companies' covert attempts to tap into the Chinese market and could result in China setting 'technological standards in parts of the world that use its equipment'.

The Royal Institute Elcano considers the Sino-American tech rivalry to pose a threat to the EU, as it leads to a massive subsidy race with unpredictable consequences. The large-scale incentives in the form of subsidies and tax breaks introduce dangerous imbalances into the global playing field. In order to catch up, the EU must rethink its state aid framework and the financing of innovation. The Institute for International Political Studies argues that, while the EU's ability to act as a normative player and technological standard-setter is important, it struggles to keep up with the US and China when it comes to industrial innovation. To strengthen the EU's capacity to develop and produce critical technologies Elcano recommends increased funding for research and innovation, as well as boosting investment in digital infrastructures.

The Centre for European Reform underlines that 'the EU acting together as a whole can match the US and China in a way that member states cannot'. However, it considers the economic security

strategy insufficient for the challenges that the EU is facing, 'largely accepting member-state competences in areas like export controls and foreign investment screening and relying on voluntary mechanisms which have failed in the past'. Instead, as recommended by Enrico Letta in his recent report on the single market, the governments should support more EU-level decisions on economic security and industrial policy, thereby reducing the influence and impacts of China or the US on individual Member States. Letta also recommends a coordinated and comprehensive EU technology policy that underpins the broad, long-term investment necessary for ambitious and costly technological development. Funding should be made available by mobilising private players through the establishment of a savings and investments union and a reform of the EU state aid rules.

The Atlantic Council welcomed the economic security strategy, calling it 'not a roadmap that will solve all of Europe's woes but an opening salvo'. The experts praised its push for more structured dialogue with the private sector and focus on adaptability and flexibility, as geopolitical circumstances are unpredictable. The key questions will be how to use the whole economic statecraft toolkit to achieve optimal results and how to engage Member States and other countries.

Conversely, the European Policy Centre warns that the ongoing global shift from a predominant model of cooperation to one of confrontation and competition may set the EU on a course towards the 'securitisation' of its policies. This could involve expanding economic security policy and tech security policy, which may gradually make the EU inwards looking and defensive on global stage.

The Carnegie Endowment for International Peace notes that the EU aims to set a gold standard for AI regulation and maintain a technological edge. However, to achieve this, the EU must effectively manage the geopolitics of AI governance in an environment that is being transformed by state and corporate competition, as well as an increasingly complex system of regulatory frameworks that are often disparate. Key actions to shape global AI governance include 'building a harmonized EU foreign policy approach to AI, fostering strategic alliances with key partners, operationalizing the AI Act effectively, and navigating diverse governance initiatives'.

The European Centre for Development Policy Management has published a set of recommendations for the EU to 'develop an approach to digital sovereignty that appeals at the international level, and can support EU digital partnerships with developing countries in the Global South'. Firstly, the EU will need to demonstrate how its policies strengthen the digital sovereignty of partner states, possibly integrating them into the EU's value chains and forming alliances based on mutual respect and genuine dialogue. Secondly, the EU will need to formulate approaches with partner countries to key concepts of its vision of digital sovereignty, such as human-centric digital transformation. Thirdly, the EU should be more flexible in its partnerships on issues such as data governance. Finally, the EU should expand its alliances. It should work with the US on joint investments in the Global South and team up at multilateral tech forums. It should also cooperate with India to promote digital public goods and infrastructure on the international stage, and with Africa towards closer integration of their digital markets and meeting the Global Gateway commitments.

The European Council on Foreign Relations (ECFR) published analysis of the EU's position at the nexus of technology and geopolitics and recommended a wide-ranging set of actions to improve it. The EU should embrace a new digital vision based on three pillars. Firstly, to establish a human rights-focused, rules-based global technological order, it should increase its bilateral and multilateral engagement with like-minded and interested countries to align on regulatory developments. It also needs to build alliances in international organisations, increase engagement and collaboration with the private sector and civil society, and clearly incorporate foreign policy objectives into EU digital policies. Secondly, to ensure the security of the EU and its partners, it should develop capabilities in emerging military and dual-use technologies and prevent their uncontrolled dissemination. Additionally, it should provide technical, financial and political support, to third countries to safeguard secure digital infrastructure and critical assets. Furthermore, it should boost cyberspace cooperation by sharing information on threats and coordinating technical and diplomatic responses to cyber-attacks, while collectively advancing global norms for secure digital technologies. Thirdly, to promote fair, open, and inclusive digital markets, the EU must increase

public and private investment connectivity in less developed countries, establish technology development partnerships based on democratic values and build alliances that advocate for a rules-based international trade system. It should also re-examine its trade agreements to find new opportunities to promote digital trade, ensure fair market access, and secure international supply chains. Additionally, the EU should explore international joint research and development opportunities in critical technologies. It could also deploy a number of new global policy tools such as a democracy protection fund, a digital rights initiative, a democratic technology standards initiative, a global cybersecurity fund, a secure technology initiative and a sanctions' monitoring and implementation initiative.

MAIN REFERENCES

Burrows M. et al., *Unpacking the geopolitics of technology*, Atlantic Council Geotech Centre, 2021.

Desautels Faculty of Management, McGill University, *The geopolitics of semiconductors and Artificial Intelligence*, World Economic Forum, 2024.

Patil S. and Mishra V., *Democracy, Technology, Geopolitics*, Observer Research Foundation, 2022.

Ringhof J. and Torreblanca J.I., *The geopolitics of technology: How the EU can become a global player, European Council for Foreign Relations*, 2022.

ENDNOTES

1 This is a ranking from Freedom of the Net Report 2023, which assessed 70 countries in six regions around the world.

2 Some experts argue that China has already overtaken the US in the high-tech supremacy race: according to the Australian Strategic Policy Institute, it is a global leader in 37 out of 44 critical technologies.

3 While submarine cables are mostly provided by France, the US and Japan, HMN, China's submarine cable leader, became the world's third-largest supplier of cables in 2022.

4 While international alignment on AI governance is emerging through forums such as the G7 and the UN, it remains a work in progress. The first binding treaty (hard law) was adopted by the Council of Europe only in May 2024.

5 The Council discussed the ASML case in its Working Party on Dual Use Goods. It also supported better coordination of national control measures in its 2024 conclusions on the white paper on export controls.

6 The EU has launched secure connectivity packages with Costa Rica, Jamaica, Kenya, the Philippines and Tunisia.

7 Furthermore, the envisaged agreements with Mexico and Mercosur have digital trade chapters, and the EU is currently negotiating digital trade chapters with Australia, India, Indonesia and the region of eastern and southern Africa (ESA).

8 Raw materials partnerships were signed with Canada and Ukraine in 2021, Kazakhstan and Namibia in 2022, Argentina, Chile, Zambia, the Democratic Republic of Congo and Greenland in 2023, and Australia, Rwanda, Norway and Uzbekistan in 2024.

9 The middle powers were Brazil, India, Israel, Japan, Kenya, Nigeria, Russia, South Korea, and the United Kingdom.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)