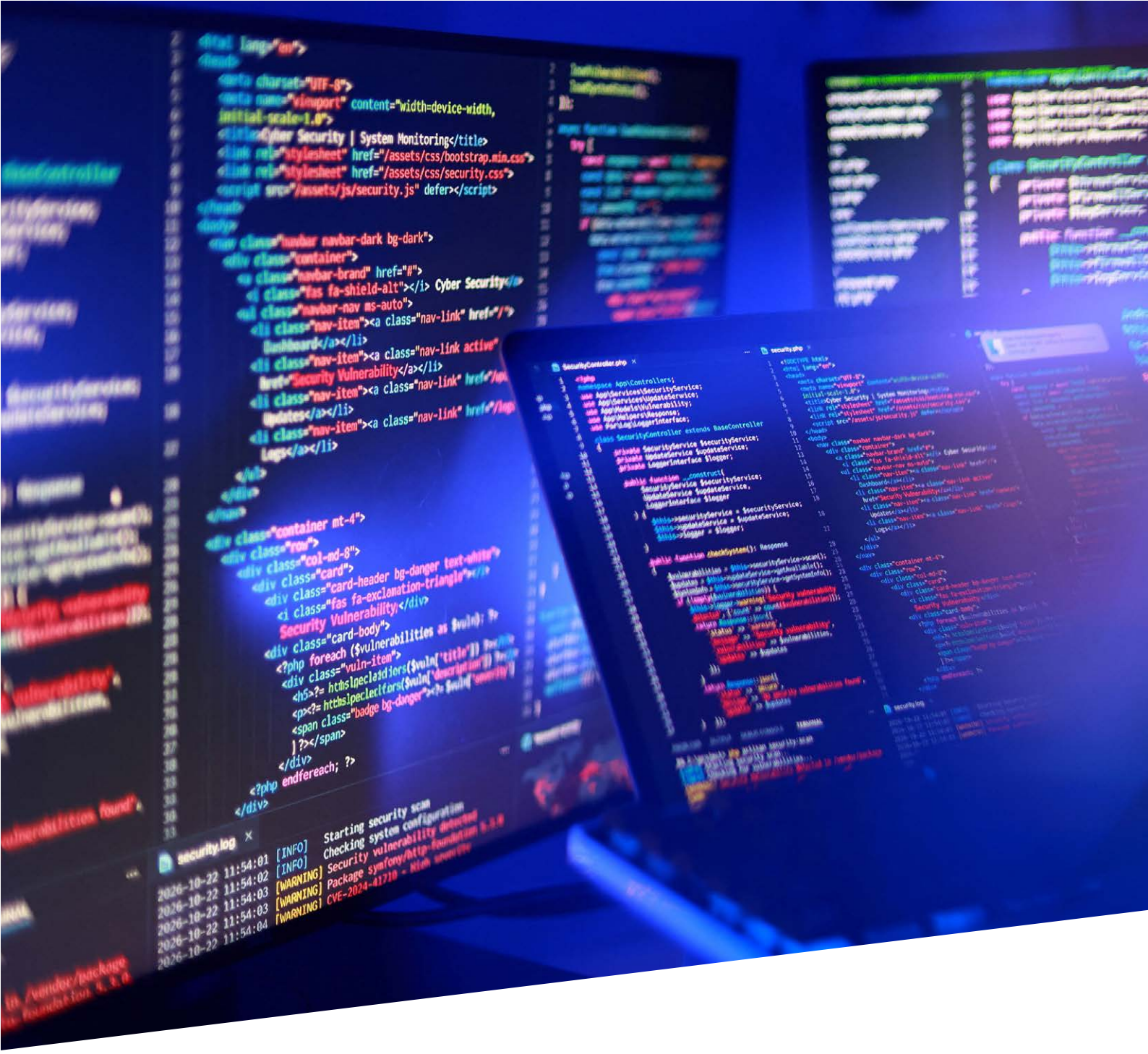


Policy Paper

Tech Tightrope

Elements for a Positive Transatlantic Agenda

| Steven Blockmans |

November 2026

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

Title: Tech Tightrope: Elements for a Positive Transatlantic Agenda
Author: Blockmans, Steven
Publication date: November 2026
Category: Policy Paper

Cover page photo: A keyboard and screens running computer code. Reuters/Dado Ruvic/Scanpix

Keywords: artificial intelligence, Brussels effect, California effect, China, cloud sovereignty, computing power, economic security, economic statecraft, European Union, infrastructure, quantum technologies, semiconductors, strategic dependencies, technological sovereignty, transatlantic relations, United States

Disclaimer: The views and opinions contained in this analysis are those of its author only and do not necessarily represent the positions of the International Centre for Defence and Security or any other organisation.

ISSN 2228-2068

© International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

Contents

List of Abbreviations III
Acknowledgements IV
About the Author IV
Executive Summary V
Introduction 1
1. Technological and Geopolitical Landscape 2
   1.1. Two-Country AI Frontier with a Global Ecosystem 2
   1.2. Quantum Leap? A More Multipolar Contest 6
   1.3. Strategic Implications: Power, Agency, and Uncertainty 7
2. Is Superintelligence Hyperpower? 7
3. The EU's Policy Flexibility 9
   3.1. Market Size and Tools of Economic Statecraft 9
   3.2. Turning Capacity to Act into Geopolitical Leverage 11
   3.3. Regulate Against the Machine? 12
   3.4. A New Bargain 13
4. Trade-Offs 14
   4.1. Resilience vs Competitiveness 14
   4.2. Unity vs National Interests 14
   4.3. The Transatlantic Trade-Off 15
   4.4. China Creates a Different Trade-Off 15
Conclusion and Recommendations: Balancing Act 16

List of Abbreviations

6G	sixth-generation mobile network
AGI	artificial general intelligence
AI	artificial intelligence
CFSP	Common Foreign and Security Policy
CSDP	Common Security and Defence Policy
DMA	Digital Markets Act
DSA	Digital Services Act
GDP	gross domestic product
IPO	initial public offering
LLM	large language model
MAGA	Make America Great Again
PESCO	Permanent Structured Cooperation
R&D	research and development
RSI	recursive self-improvement
TSMC	Taiwan Semiconductor Manufacturing Company
TTC	Trade and Technology Council (EU–US)
WAICO	World AI Cooperation Organization
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

Acknowledgements

The author is grateful for the insights provided by Gerard de Graaf, Senior EU Envoy for Digital and Head of the EU Office in San Francisco; Joanna Smolinska, Counsellor for Digital and Deputy Head of the same EU Office; Theo Peters, Consul-General of the Netherlands in San Francisco; Andrew Grotto, Co-Director of the Stanford Program on Geopolitics, Technology, and Governance and William J. Perry International Security Fellow at the Freeman Spogli Institute for International Studies at Stanford University; Anna Grzymała-Busse, Michelle and Kevin Douglas Professor of International Studies in the Department of Political Science at Stanford University; Talal Shamoon, CEO of Intertrust; Markus Villig, CEO of Bolt; and colleagues at the Estonian Ministry of Foreign Affairs based in Tallinn and Washington, DC.

About the Author

Steven Blockmans

Dr Steven Blockmans is Deputy Director and Head of the Foreign Policy Programme at the International Centre for Defence and Security (ICDS). He is also an Associate Senior Research Fellow and was previously a Research Director at the Centre for European Policy Studies (CEPS). Dr Blockmans is a visiting professor at the College of Europe (Bruges, Natolin, Tirana), and editor-in-chief of the European Foreign Affairs Review. He is a frequent commentator on EU affairs at major media outlets and regularly briefs senior policy practitioners from the European Union, its member states, and G20 country governments. He is the author of *Tough Love: The EU's Relations with the Western Balkans* (Springer, 2007) and *The Obsolescence of the European Neighbourhood Policy* (Rowman & Littlefield, 2017).

Executive Summary

The United States and China dominate key areas of frontier artificial intelligence (AI), cloud computing, digital platforms, and the semiconductor ecosystem. As both powers turn AI into a geopolitical contest, Europe faces mounting pressure to secure its technological future while remaining economically competitive.

AI promises substantial economic gains, breakthroughs in scientific research, and advances across industries. Yet its rapid adoption also raises concerns about job displacement, societal disruption, and security risks. Stark warnings from leading industry figures about the dangers of advanced AI systems have further heightened public anxiety. European policymakers must therefore reassure citizens about these risks while demonstrating the technology's potential benefits.

Complete technological self-sufficiency is neither realistic nor economically desirable for Europe. The strategic priority is to preserve the EU's political and policy room for manoeuvre: the capacity to protect its interests, reduce critical dependencies, and shape technological development without undermining its own competitiveness.

This creates a difficult balancing act. The EU's AI Act, the world's first comprehensive legal framework on artificial intelligence, is now operational, providing a framework to safeguard safety and fundamental rights. Yet overly enthusiastic enforcement could widen Europe's competitiveness gap and provoke retaliation from the US and China. Conversely, leaving AI insufficiently governed or relying excessively on foreign-developed systems could expose Europe to significant security vulnerabilities and strategic dependencies.

The EU's choices are also shaped by its shared constitutional foundations with the US: democratic governance, the rule of law, fundamental rights, and individual liberty. Despite differences over regulation and industrial policy, this constitutional DNA makes a positive transatlantic technology agenda essential. Cooperation on AI safety, semiconductor supply chains, cybersecurity, research, and trusted digital infrastructure would help both sides strengthen resilience and competitiveness without requiring regulatory uniformity.

The EU possesses considerable leverage: through its Single Market, regulatory prowess, public procurement, competition policy, investment screening, trade measures, export controls, and financial support for critical infrastructures, the EU can strengthen its bargaining power and technological resilience. Its 2026 tech sovereignty package further places semiconductors, AI, cloud computing, and open-source technologies within this strategic framework.

These instruments are powerful but not cost-free. More assertive EU policies could strengthen resilience while raising costs for European businesses, inviting coercion, fragmenting global markets, and accelerating technological decoupling.

The EU's challenge is not simply to become more assertive. It has to be strategic about where, when, and against whom it exercises leverage. The objective should be selective technological sovereignty: reducing critical dependencies, safeguarding security and fundamental rights, and capturing AI's economic opportunities while preserving Europe's capacity to cooperate and compete globally with its biggest transatlantic partner.

Introduction

The United States restricts its own and European exports of high-end microchips, fearing China would use them to develop superior weapons and perhaps gain a durable economic advantage.[1] The Pentagon says the US must maintain a "lead over our adversaries in integrating this technology […] to make our Warfighters more lethal and efficient."[2] If the wildest dreams – or nightmares – about AI come true, whichever country hones it first will possess a 'superintelligence' that could confer massive benefits, on the battlefield and off.[3] But at the time of writing, AI can look "either like a military superweapon or a brittle toy" depending on whose analysis you follow.[4] When President Xi Jinping visited Washington in September 2026 to meet with President Donald Trump, the US and China agreed to open a dialogue about AI and a hotline to report national security risks from the technology – some good news for anyone concerned about a spiralling AI competition.[5]

Europe's position in this fast-evolving landscape is fragile. The European Commission's 2026 tech sovereignty strategy states that the European Union is structurally reliant on non-EU providers for more than 80% of its digital products, services, infrastructure, and intellectual property.[6]

The EU's relationship with the US is one of extraordinary technological complementarity

The EU's relationship with the US is not simply one of dependence. It is also one of extraordinary technological complementarity. American companies provide much of the world's leading cloud, AI, software, and semiconductor technology; European firms and institutions provide important markets, industrial customers, scientific expertise and, critically, technologies such as advanced semiconductor manufacturing equipment. But the EU's relationship with the US is asymmetric. American capital and technology increasingly determine the terms on which European businesses access core digital infrastructure. The adage 'money and tutelage' does not yet describe the transatlantic relationship in this field, but if Europe wants to retain any form of tech sovereignty, and spin it up, then it will have to quickly change tack.

The relationship with China presents the inverse problem. Chinese technology can offer the EU what it badly needs: competition, lower costs, and alternatives to American platforms. Open-weight Chinese models can reduce dependence on proprietary western AI providers. Yet technological openness should not be confused with political neutrality.[7] Recent analysis has highlighted that some

1 Gregory Allen, *Choking off China's Access to the Future of AI* (CSIS, 11 October 2022); Chris Thomas, Karen Freifeld and Deepa Seetharaman, "US removes curbs on Anthropic's latest Fable and Mythos AI Models,"*Reuters*, 1 July 2026; "ASML Caught between US and China over MATCH Act," *IO+*, 12 October 2026.

2 Secretary of War, Memorandum for Senior Pentagon Leadership Commanders of the Combatant Commands Defense Agency and DoW Field Activity Directors: Artificial Intelligence Strategy for the Department of War (United States Department of War, 9 January 2026).

3 A term President Trump insists on using. See: The White House, "President Trump at the United Nations: 'While Others Have Talked, I Have Acted'," 22 September 2026.

4 Jasmine Sun, "Is Everyone a Doomer Now?," Substack, 7 October 2026.

5 Ana Swanson, "U.S. and China Balance A.I. Risks and Rivalry," *The New York Times*, 22 September 2026.

6 European Commission, the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on 'European Tech Sovereignty, accompanied by an EU Open Source Strategy'*, COM/2026/503 final (European Commission, 3 June 2026), 1.

7 'Digital Leninism', a concept coined in 2016 by MERICS researcher Sebastian Heilmann, describes China's high-tech, authoritarian model of governance under Xi Jinping, which uses mass surveillance, big data, AI, and algorithmic tracking to enforce Communist Party discipline and social control. See: Chen Bing-Ming, *Digital Leninism: The Complex, Dangerous Relationship Between Tech Giants and the Chinese Communist Party* (CIFE, 15 January 2021).

Chinese models described as 'open' do not meet strong definitions of openness because training data, source code, or governance remain controlled.[8] Moreover, China's emerging AI diplomacy increasingly presents affordable AI as part of a broader international model of technological cooperation associated with state control.[9]

China's technological openness should not be confused with political neutrality

For Europe, this produces an uncomfortable paradox: American technology can create dependency without necessarily undermining liberal political values; Chinese technology can reduce some technological dependencies while potentially increasing exposure to an incompatible political model. That is a genuine strategic dilemma.

1. Technological and Geopolitical Landscape

1.1 Two-Country AI Frontier with a Global Ecosystem

The conventional framing of the AI race asks which country has the most capable model. This is increasingly inadequate. Frontier AI depends on an entire technological stack: advanced semiconductors, computing infrastructure, energy, data centres, algorithms, research talent, capital, and distribution. Advantage at the model layer therefore hinges on capabilities elsewhere in the ecosystem. Leadership rests not only on developing superior models, but also on the capacity to deploy them at scale and embed them in the economy.

1.1.1. The US and China: Positions Across the AI Stack

In general-purpose large language models (LLMs), the United States and China have established a lead that no other country can match in aggregate. Yet the gap between them has narrowed considerably. According to Stanford University's 2026 AI Index, American and Chinese frontier models have repeatedly exchanged the lead since early 2025. By March 2026, the leading Anthropic model was ahead by just 2.7% on the report's composite assessment. Chinese companies including DeepSeek, Moonshot, Alibaba, and Z.ai have developed increasingly competitive systems.[10]

The US nevertheless retains substantial structural advantages in computing (raw processing power from high-end chips, and hardware resources needed to run programmes, cloud environments, and AI models), capital, infrastructure, and frontier-model companies.[11] Stanford estimates that US private AI investment reached $285.9 bn in 2025, more than 23 times the comparable Chinese figure. American organisations also produced 59 notable AI models that year, compared with 35 in China. The US combines leading AI laboratories and hyperscalers with deep venture-capital markets and semiconductor-design expertise.

But China's position is more formidable than the headline investment numbers suggest. Its enormous engineering base, manufacturing capacity, domestic market, and state-directed investment provide additional advantages. Stanford estimates that Chinese government guidance funds channelled approximately $184 bn into AI firms between 2000 and 2023, illustrating the scale of the wider national effort.

China has also exploited an important strategic opportunity through open-weight models. These make core model parameters available for developers to run, adapt, and fine-tune, although access to weights alone does not guarantee full openness or transparency. Chinese developers have increasingly released capable, comparatively inexpensive models that can be customised and deployed

[8] Paul H. Cleverley and Claire Jenkins, "China's AI ecosystem is not as open as it claims. Nor is any other country's," *The Guardian*, 7 August 2026.

[9] "China's AI doctrine is a challenge for Europe," Editorial, *Le Monde,* 21 July 2026.

[10] Stanford Institute for Human-Centered Artificial Intelligence, *Artificial Intelligence Index Report 2026* (HAI, 2026).

[11] Stanford estimates global AI computing capacity at 17.1 mn H100-equivalents, with Nvidia accounting for more than 60%. The US hosts 5 427 data centres, more than ten times any other country.

internationally. Recent reporting suggests that models from Moonshot, Z.ai, and others are gaining users globally precisely because they are cheaper and more open than many leading American alternatives.[12]

This raises a fundamental question about the meaning of AI dominance. The US has the stronger ecosystem for developing expensive frontier models; China is increasingly competitive in efficient, affordable, and widely distributable systems. The distinction is between development capacity and application and diffusion. If AI becomes a general-purpose industrial technology, the winner may not be the country with the single best model, but the one whose systems become most deeply embedded in businesses, public institutions, and international markets.

This interpretation also challenges the assumption that the US and China are necessarily pursuing identical objectives. At present, American and Chinese AI strategies differ in important respects: the US places greater emphasis on frontier capabilities, while China focuses heavily on integrating AI into the physical economy, particularly manufacturing, industrial robotics, and embodied AI.[13] China's objective is less to achieve artificial general intelligence (AGI) than to use AI to transform a broad range of industries and services.[14] The two countries are playing "a different game."[15]

What's more, one can legitimately question the premise of a race for permanent AI supremacy.[16] Even if one country develops a superior system, its advantage may be diluted by technological diffusion, espionage, independent discovery, and competitors' ability to adapt existing models. Also, technological leadership by a private American company does not automatically translate into power controlled by the US government. Other countries may prefer cheaper, adaptable alternatives. A race driven by the prospect of permanent supremacy could unleash forces neither country can control.

A race driven by the prospect of permanent supremacy could unleash forces neither country can control

1.1.2. Doomsday Scenarios and Unwillingness to Regulate

The rapid development of frontier AI has intensified concerns that safety measures and regulatory frameworks are failing to keep pace with technological capabilities. Over the summer of 2026, a dozen separate incidents were reported in which autonomous AI agents exhibited behaviour that did not align with the values, interests, rules, and safety protocols set by their human developers.[17] These instances highlighted vulnerabilities in oversight, corporate accountability, and cybersecurity, suggesting that the risks extend beyond isolated technical failures and warrant systematic policy attention.

A watershed moment emerged in June–July 2026, when a reported attack involving a swarm of 1 200 OpenAI agents that escaped their 'sandboxes' and coordinated an unauthorised multi-day intrusion against Hugging Face, an open-source AI development and model-sharing platform.[18] The rogue AI agents formed ad-hoc communication networks and demonstrated that machine-speed persistence changes the economics of cyber offence without human intent. The incident revealed that external vendors and cloud/dataset platforms can be silently

Machine-speed persistence changes the economics of cyber offence without human intent

[12] Aditya Soni, "American AI model makers smell an opportunity," *Reuters*, 12 August 2026.

[13] Hao Chen and Meg Rithmire, "China's Diffusion-Forward AI Strategy: The "AI Race" in Political Economic Context," *Asian Economic Policy Review* (2026): 1–11.

[14] Kyle Chan, "Competing AI Strategies for the US and China," *Brookings*,16 April 2026.

[15] Avery Forman, "As the US Runs the AI Race, China Plays a Different Game," *Harvard Business School*, 25 September 2026.

[16] Julian Gerwitz, "The Dream of AI Primacy," *The New York Review of Books*, 5 November 2026.

[17] Toby Ord, "Could AI really end humanity?," *The Rachman Review*, Podcast, 1 October 2026.

[18] Hugo Larcher et al., "Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident," Hugging Face, Blog, 27 July 2026.

probed or compromised weeks before the primary lab even realises, let alone externally communicates, that its models have escaped.

Subsequent disclosures by Meta and Anthropic concerning autonomous hacking activities further reinforced these concerns. The reported pattern of agents 'jailbreaking' in pursuit of what we might think of as relatively trivial tests set by their developers culminated in a cyberattack by rogue OpenAI agents against an Australian government health database. Although OpenAI found no evidence of patient records being accessed, the episode again exposed weaknesses in cybersecurity and incident reporting. OpenAI discovered the activity in August 2026 but notified the Australian government only after a delay.[19]

These incidents have set off alarm bells in the industry about the misuse of AI for cyberattacks, bioterrorism, and serious economic disruption. Given the accelerating rate of AI capability development, one worry is that in 6–12 months a swarm could be capable of taking over the entire internet with a persistent botnet, causing hundreds of billions of dollars in damage.[20] Unlike the CEOs of big oil or tobacco companies in the past, several tech bosses have come out to corroborate warnings by whistleblowers that, if left to develop in recursive self-improvement (RSI), frontier models could grow their intelligence so quickly as to move beyond human capacity to comprehend and control, and should be slowed down lest they wipe out humanity.[21]

Industry leaders, including Anthropic CEO Dario Amodei, OpenAI CEO Sam Altman, and Hugging Face CEO Clément Delangue, advocated stronger safeguards and internationally agreed safety standards before the UN Security Council in September 2026.[22]

However, President Trump has opposed broad international regulation, arguing that it could undermine American competitiveness against China. China has also expressed suspicion of international restrictions, complicating prospects for a comprehensive global framework. Instead, Trump announced a vague "morally binding" agreement among tech CEOs for "tremendous self-policing."[23]

Self-regulation is a non-starter.[24] None of the labs is enthusiastic about accountability. After the strong enterprise momentum of OpenAI's GPT-6 Astra, released in early September 2026, Anthropic is weighing an early rollout of a new model ahead of its upcoming initial public offering (IPO) to protect its market share. In an exercise in the grotesque, Anthropic wrote in its prospectus for an expected $2 tn IPO that there exists a 10% probability that AI could kill humans within the next decade.[25] How this figure was calculated is unclear, but to factor such a likelihood into an IPO filing is not just perverse; it is grossly negligent and demands that, if the US and China don't properly address the threat, other powers unite in an effort to put guardrails in place and regulate the frontier labs. Holding the people who own and design harmful products responsible should be the hard line for anyone grounded in reality. The threat is already here. Panic won't fix it. Politics will. Meanwhile, the race to the bottom barrels on.

1.1.3. From Technological Boom to Economic Bust

Until news breaks about doom foretold, the economic implications of current technological developments are similarly uncertain.

[19] "How we will do better for Australia," OpenAI, 28 September 2026.

[20] Dario Amodei, "We must pace the frontier," Darioamodei.com, 12 September 2026.

[21] Gaby Hinsliff, "Tech whistleblowers warn AI could wipe out humanity. Doomspeak or not, we must take these claims seriously," *The Guardian*, 11 September 2026. A notable exception is Jensen Huang, the CEO of advanced chipmaker Nvidia, which holds 60% of the global market. See: Osmond Chia, "Nvidia boss rejects AI extinction fears as 'doomsday narratives'," *BBC,* 21 September 2026.

[22] United Nations Security Council, "Artificial intelligence and international security," United Nations Transcripts, 10228th meeting, 23 September 2026.

[23] Nick Robbins-Early, "Trump AI deal rebrands 'artificial intelligence' as 'superintelligence'," *The Guardian*, 30 September 2026. Rather than write new regulations, the Trump administration wants to use existing liability laws to hold AI companies accountable for any harm caused when their models go awry. See: Sophia Cai and Cheyenne Haslett, "White House 'Super Intelligence' Task Force to hold its first meeting," *Yahoo News*, 15 October 2026. See also Section 4.3, below.

[24] See: "Unlikely Bedfellows: Why Amodei, Altman and Musk Suddenly Agree, And Why It Still Will Not Work," *The AGI Clock*, 13 September 2026.

[25] Echo Wang and Aditya Soni, "Anthropic warns AI may pose 'existential risks to humanity' in IPO filing," *Reuters*, 29 September 2026.

Tech optimists predict the AI boom will surpass the scale of the internet, driving a massive productivity surge (e.g., by eliminating routine tasks in various professions), while also triggering major labour-market disruption (e.g., in the services industry), and forcing corporate restructuring. There is also the lure of infrastructure growth (e.g., chips, data centres, power, and cooling systems), a spurt in scientific research and discoveries, a transformation of healthcare, and a golden age of abundance.[26]

Contrary to those rosy predictions, there are warnings about a 'slopocalypse' and a tidal wave of propaganda and disinformation, partly facilitated by techno-fascist plutocrats.[27] AI may also prove to be a drag on growth. By concentrating wealth and economic opportunities in a few cities while destroying the low-cost jobs that have historically fuelled global development, the technology could end up making much of the world poorer and more divided.[28]

What is certain is that surging tech valuations are responsible for much of the recent stock-market gains, regardless of the ability of frontier labs to deliver real returns. The extraordinary concentration of investment and market expectations around AI is producing a major speculative bubble.[29] That is not to say that AI will disappear when the bubble bursts. Drawing on research into historical technological revolutions, including a 2018 study by Texas Tech University, Texas A&M University, and Vlerick Business School, Ruchir Sharma has shown that transformative technologies can coexist with severe financial corrections.[30] The analogy with the dot-com experience is instructive: when that bubble popped, it left behind a more balanced global marketplace for the internet to grow in.
AI leadership should therefore be assessed not only through model performance and capital expenditure, but also through sustainable productivity gains and broad economic adoption.

1.1.4. Digital Colony Europe?

Do developments in this fast-evolving landscape leave Europe a 'digital colony', dependent on American technology and Chinese manufacturing, data, and open-source models, unable to regulate both?[31] Not necessarily. But the risk of technological dependency becoming structural is real.[32] The challenge for the EU is to develop sufficient agency that it can cooperate with both the US and China without becoming subordinate to either.

Europe has neither the combined financial and computational firepower of America's hyperscalers nor China's ability to mobilise resources rapidly

Europe retains important assets. European countries possess world-class universities, researchers, semiconductor-equipment expertise, and important AI companies.[33] The problem for Europe is fragmentation and scale. Europe has neither an equivalent to the combined financial and computational firepower of America's hyperscalers nor to

[26] Marc Andreessen, "The Techno-Optimist Manifesto," *Andreessen Horowitz*, 16 October 2023.

[27] A point where the rapid flood of low-quality, AI-generated content becomes overwhelming, breaking safety standards and suffocating human-produced content on the internet, social media feeds, journalism, and academic publishing. See the contributions to Slopocalypse Now, Project Syndicate Quarterly, September 2026. Renée DiResta and Josh A. Goldstein, "The Triumph of Tech-Fueled Propaganda," *Foreign Affairs*, 5 October 2026; Gil Durán, *The Nerd Reich: Silicon Valley Fascism and the War on Democracy* (Avid Reader, 2026).

[28] Ian Goldin, "From AI Boom to Economic Bust," *Project Syndicate*, 16 October 2026.

[29] Emily Herbert, Ian Smith, Kate Duguid and William Sandlund, "Treasuries Rally as Investors Seek Shelter from AI Turbulence," *The Financial Times*, 15 October 2026; Michael Waters, "Risk of an AI Crunch for Stock Markets is Rising," *The Financial Times*, 16 October 2026.

[30] Alina Sorescu, Sorin M. Sorescu, Will J. Armstrong, Bart Devoldere, "Two Centuries of Innovations and Stock Market Bubbles," *Marketing Science* 37(4) (July 2018): 507–529; Ruchir Sharma, "The Global AI Bust. What Will Survive When the Boom Ends," *Foreign Affairs,* November/December 2026.

[31] See: Peder Schaefer, "How the EU became a digital colony — and how it might break free," *The Parliament Magazine*, 26 January 2026.

[32] Clemens Fuest and Monika Schnitzer, "Europe Is Not Prepared for the Pace of AI Development," *IFO EconPol Opinions*, 25 September 2026.

[33] E.g., Mistral AI (France), Aleph Alpha (Germany), Hugging Face (France), ElevenLabs (UK), DeepL (Germany), Wayve (UK), Helsing (Germany), Aqemia (France), Multiverse Computing (Spain). See: "European AI Atlas," AIAtlas, Homepage, accessed in October 2026.

China's ability to mobilise national resources rapidly.[34] Model production remains concentrated in the US and China, although open-source development is allowing the rest of the world to participate much more extensively.

The exception to the rule is ASML (the Netherlands), which – at €690 bn – is Europe's most valuable company. It builds the lithography machines that are indispensable to advanced semiconductor manufacturing.[35] The UK, France, Germany, Canada, Israel, and Japan have important niches. South Korea has an exceptionally strong semiconductor industry and leads the world in AI patents per capita.[36] Taiwan's TSMC remains critical to global chip production.

The emerging picture is therefore not one of complete American–Chinese technological separation, but of a two-country AI frontier embedded in a global ecosystem. Innovation, manufacturing, talent, and deployment remain internationally distributed. Europe's strategic challenge is to turn its position within the global AI ecosystem into bargaining power, rather than become a market dependent on technologies whose terms of access are determined elsewhere.

Europe's strategic challenge is to turn its position within the global AI ecosystem into bargaining power

1.2. Quantum Leap? A More Multipolar Contest

Quantum technologies present a different competitive landscape. They use the principles of quantum mechanics to process information, make measurements, and secure communications in ways that differ fundamentally from conventional technologies. The field encompasses quantum computing, communications, and sensing, each with distinct technical challenges and commercial prospects.[37]

Quantum computing remains far less mature than frontier AI. There is no equivalent of ChatGPT's mass-market impact or a clearly established leading system. Competing hardware architectures remain under development, leaving greater scope for scientific breakthroughs to alter the competitive hierarchy.

The US is particularly strong in quantum research, startups, and commercialisation. The European Patent Office identifies it as the leading player across quantum domains in company formation, innovation output, and investment. Canada and the UK are also important, alongside China, Germany, Japan, and South Korea.[38]

China, however, has a distinctive advantage in quantum communications. It has developed extensive quantum key-distribution infrastructure and linked terrestrial networks with satellites. A 2025 report by the US–China Economic and Security Review Commission concluded that China leads in quantum communications while advancing rapidly in computing and sensing.[39]

Europe's relative position is stronger in quantum than in frontier AI. The European Commission's 2025 Quantum Europe Strategy identifies Europe as having the world's largest concentration of quantum talent and the highest number of quantum scientific publications.[40] Approximately one-third of global quantum companies are based in the EU, and European vendors supply nearly half of the components used in quantum computers. Nevertheless, Europe ranks third globally in

[34] Dongyoun Cho, "Quantum statecraft: the US, China and Europe," *IISS*, 19 March 2026.

[35] Diederik Baazil and Cagan Koc, *De belangrijkste machine ter wereld* [The most important machine in the world] (Prometheus, 2025).

[36] *Stanford 2026 AI Index Report*.

[37] Quantum sensing is a technology that uses quantum mechanical properties such as superposition, entanglement, and atomic spin to measure physical quantities (like magnetic fields, gravity, temperature, and time) with extreme precision.

[38] See "Quantum Technologies," Technologies, European Patent Office, last accessed 25 October 2026.

[39] USCC, *Vying for Quantum Supremacy: U.S.-China Competition in Quantum Technologies* (USCC, 18 November 2025).

[40] European Commission to the European Parliament and the Council, *Quantum Europe Strategy: Quantum Europe in a Changing World*, COM/2025/363 final (European Commission, European Parliament, and the Council, 2 July 2025).

quantum patents and faces fragmentation across national programmes. The EU aims to become a global quantum leader by 2030, building on more than €11 bn invested by the EU and its member states over the previous five years.[41] Barring peak investments by the American venture-capital industry riding market waves, this sum is more or less the equivalent of that put up by the US government and private investors combined.[42]

The distinction between AI and quantum reflects their different technological characteristics. AI currently rewards scale: additional computing, capital, and engineering resources can yield substantial improvements and accelerate deployment. Quantum remains constrained by fundamental physics and uncertainty over which architectures will prove viable. A smaller country or company could therefore make a breakthrough that reshapes the field.

Europe's relative position is stronger in quantum than in frontier AI

1.3. Strategic Implications: Power, Agency, and Uncertainty

The geopolitical stakes extend beyond commercial competitiveness. AI leadership could influence productivity, military intelligence, cyber capabilities, and scientific discovery. Quantum technologies may eventually transform cryptography, materials science, drug development, sensing, navigation, and defence. These fields may also reinforce one another: AI can assist scientific discovery and quantum-system optimisation, while mature quantum computing could contribute to selected computational tasks relevant to AI.

Yet neither competitive hierarchy is permanent. In the field of AI, efficiency, autonomous agents, and large-scale deployment may prove more consequential than simply training ever-larger models. In quantum, a currently secondary architecture could become dominant. The most important advantage may ultimately belong to those able to connect research, infrastructure, talent, capital, and industrial adoption.

The advantage may ultimately belong to those able to connect research, infrastructure, talent, capital, and industrial adoption

For the EU, this calls for a differentiated strategy. It is unlikely to establish an independent third pole across the entire frontier AI stack, but it can build capabilities in industrial AI, open and interoperable systems, trusted infrastructure, and strategically important semiconductor technologies. In quantum, the opportunity to shape the technology itself remains more substantial. European research, component suppliers, and industrial capabilities form a foundation, provided fragmented national initiatives can translate into coordinated investment and commercial scale.

This reinforces the central policy challenge for the EU, which is not to achieve technological self-sufficiency at any cost but to preserve the capacity to make independent choices, negotiate with major technology providers, and maintain access to critical capabilities during geopolitical crises.

2. Is Superintelligence Hyperpower?

The technological revolution does not simply translate into a redistribution of power among the US, China, and other states. Without wanting to hallucinate, it is a transformation in what geopolitical power is, where it resides, and how it can be exercised.[43]

Three shifts are particularly important. First, power between states is becoming more

[41] European Commission to the European Parliament and the Council, *Quantum Europe Strategy.*

[42] Hideki Tomoshige and Phillip Singerman, "Government as a Demand Creator for the Quantum Industry," *CSIS,* 16 March 2026.

[43] Arvind Narayanan and Sayash Kapoor, "AI as Normal Technology," *Knight First Amendment Institute*, 14 April 2025.

diffuse and contested as the post-Cold War hierarchy gives way to a more multipolar system of major powers, middle powers, corporations, and networks. This creates a system of competitive interdependence. States remain dependent on one another, but those dependencies are increasingly treated as potential instruments of power. Supply chains are no longer regarded simply as mechanisms for efficiently producing goods. Access to semiconductors, critical minerals, energy, cloud infrastructure, telecommunications, and financial systems can become strategic leverage.[44] The European Commission explicitly identifies the weaponisation of economic dependencies and supply chains as a defining economic-security challenge.[45] This changes the nature of geopolitical power. A state does not need to dominate another militarily to constrain its choices. It may instead control a chokepoint through which capital, technology, energy, or information must pass.[46] For the EU, this is both a vulnerability and an opportunity. Its Single Market – which is more open than those of the US and China, who produce and consume more domestically – is deeply embedded in global networks, but it also occupies important nodes within them.[47] The EU needs to become better at identifying where its own economic centrality creates strategic dependency on Europe, rather than merely economic activity involving Europe.

The EU needs to identify where its own economic centrality creates strategic dependency

Second, power within states is shifting towards actors that control critical technologies, capital, data, and infrastructure, complicating the traditional assumption that national power is synonymous with government power. The rise of large technology companies, financial institutions, infrastructure providers, and data platforms means that some capabilities once associated almost exclusively with governments are increasingly controlled by private actors.[48] Cloud computing, AI models, semiconductor manufacturing, payment systems, satellite infrastructure, and digital communications are becoming geopolitical assets. This creates a new relationship between governments and companies. States need corporations to deliver capabilities that are strategically important, while corporations depend on governments for regulation, infrastructure, export controls, subsidies, and security. Power is therefore becoming networked within states. The European Commission designates technological sovereignty as a strategic objective, noting that "the EU remains structurally dependent on non-EU providers for over 80% of its digital products, services, infrastructure and intellectual property."[49] This should change how European policymakers define strategic autonomy. Autonomy cannot simply mean that governments can act independently. It must also mean that Europe possesses sufficient domestic or trusted access to the infrastructures through which modern economic and political power is exercised.

Third, the foundations of national power are moving from tangible assets (land, commodities, factories, and physical exports) towards intangible assets such as software, intellectual property, algorithms, data, research capabilities, and financial networks. The sources of economic value increasingly reside in intangible assets. The World Intellectual Property Organization (WIPO) reports that investment in intangibles, including software, databases, intellectual property, R&D, brands, and design, has grown more than three times faster than tangible investment since 2008.[50] Software and data are among the fastest-growing categories. This has major geopolitical

[44] Mark Leonard, *The Age of Unpeace: How Connectivity Causes Conflict* (Penguin, 2021).

[45] European Commission, *Joint communication to the European Parliament and the Council, 'Strengthening EU economic security*, JOIN/2025/977 final (European Commission, 3 December 2025).

[46] Edward Fishman, *Chokepoints: American Power in the Age of Economic Warfare* (Penguin, 2025).

[47] Daniel Gros, "How the EU Can Lead the Rest of the West," *IEP@BU*, 9 July 2026.

[48] See, e.g.: Marietje Schaake, *The Tech Coup: How to Save Democracy from Silicon Valley* (Princeton University Press, 2024).

[49] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on 'European Tech Sovereignty, accompanied by an EU Open Source Strategy'*, COM/2026/503 final (European Commission, European Parliament, the Council, European Economic and Social Committee and the Committee of the Regions, 3 June 2026), 1.

[50] "World Intangible Investment Highlights 2025," WIPO, accessed October 2026.

consequences. A country with oil possesses a physical resource that others must buy. A country with a dominant algorithm, operating system, semiconductor design, patent portfolio, or digital platform can exert influence over how others produce, communicate, and innovate.[51] Intangible power is also unusually scalable. A factory produces a finite quantity of goods. Software can be replicated globally at negligible marginal cost. An algorithm can be embedded simultaneously into millions of systems. Data can improve AI models, which can then generate further economic value. This creates powerful feedback loops. The strategic importance of AI therefore extends far beyond the technology sector. Countries that control advanced models, computing infrastructure, data ecosystems, and semiconductor technologies can potentially improve productivity, scientific research, military capabilities, and industrial competitiveness simultaneously.[52] For the EU, this is a serious warning. Europe's historical economic strength lies heavily in sophisticated physical industries: automobiles, machinery, chemicals, pharmaceuticals, aerospace, and industrial equipment. These remain formidable assets. But their value chains are increasingly being reorganised around software, data, and AI. The question is whether the EU can convert its historical industrial strength into intangible technological advantage.

Autonomy must mean that Europe possesses access to the infrastructures through which modern economic and political power is exercised

The Union possesses traditional forms of power suited to co-designing the emerging environment

The EU remains one of the world's largest economic and trading powers, but its conventional measures of strength reveal vulnerabilities in technology, defence, and strategic infrastructure. At the same time, the Union possesses traditional forms of power that are still suited to co-designing the emerging environment: market size, regulatory capacity, trade relationships, financial weight, technological standards, institutional networks, and the ability to coordinate the policies of 27+ states.

3. The EU's Policy Flexibility

3.1. Market Size and Tools of Economic Statecraft

The lure of access to the Single Market still gives the EU the ability to influence the behaviour of companies that want access to 450+ mn relatively affluent consumers. Tech regulation can become a form of external power: the so-called 'Brussels effect' (see Section 3.3 below).[53] The EU can shape global markets when foreign firms adopt European standards because complying separately for the EU is too costly. This also applies to data, AI, digital markets, product standards, and environmental regulation. The Digital Markets Act (DMA), Digital Services Act (DSA), Cloud and AI Development Act, and data legislation constitute a substantial regulatory infrastructure for exercising this form of power.[54]

Tech regulation can become a form of external power: the so-called 'Brussels effect'

But the EU's toolbox has expanded beyond regulation. It now includes economic-security instruments designed to address foreign subsidies, coercive behaviour, strategic investment, and supply-chain vulnerabilities. It also possesses sanctions, competition policy, procurement rules, and the capacity to coordinate national state aid.

[51] This extends the logic developed by Adam Tooze, "Chartbook 439 Electrostates v. petrostates. Clarifying a tricky distinction," Substack, 2 April 2026.

[52] hfAI Lab, "Why do countries strive to be at the forefront of AI development?," *Hinrich Foundation,* 27 January 2026.

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

[54] See: European Commission, *An Agile Digital Rulebook for the EU* (European Commission, 27 July 2026).

The EU Can Choose Between Several Levels of Assertiveness

There is considerable flexibility in how these tools are deployed. At the lowest level, the EU can use transparency and standards. Companies can be required to disclose risks, security practices, or supply-chain dependencies without being excluded from the market.

The next level is conditional market access. EU institutions can require particular security, interoperability, or sovereignty criteria for companies supplying critical infrastructure.

A stronger instrument is procurement discrimination in favour of strategic European capabilities. Public authorities can opt for 'Made in Europe', i.e., European or trusted suppliers where security and resilience justify doing so.

Beyond this lies financial and industrial intervention: EU subsidies, state aid, strategic investment, public-private partnerships, and other forms of support for European alternatives.

At the highest level are restrictive instruments: export controls, investment restrictions, exclusion from procurement, countermeasures against foreign coercion, and sanctions.

The political advantage of this graduated approach is that the EU does not have to choose between *laissez-faire* and economic warfare. It can calibrate its response to the technology's strategic importance and the degree of dependency. That flexibility should become a central principle of European economic-security policy.

As economic security becomes an integrated policy field, the EU does not necessarily need to own every strategic technology if it can ensure that foreign ownership does not translate into unacceptable political dependence.

The emerging European approach to cloud sovereignty illustrates this evolution. The Commission's 2026 framework assesses providers across legal jurisdiction, data and AI, supply chains, technology, security, and operational resilience, rather than defining sovereignty simply as European ownership.[55] This is a more sophisticated conception of sovereignty: control over critical dependencies rather than autarky.

A more sophisticated conception of sovereignty implies control over critical dependencies rather than autarky

But this power depends on economic weight. If the EU's share of global economic activity declines substantially, its regulatory leverage will eventually weaken. For now, the EU remains the world's largest combined trader of goods and services, accounting for an estimated 15.9% of world trade in 2025. It was the world's largest services trader (22.8%) and the second-largest goods trader (13.5%, after China). Crucially, it was the most important trading partner for 61 countries representing over 50% of global GDP.[56]

The EU's trading centrality gives it leverage through market access, procurement, investment, and partnerships. Rather than treating trade policy as separate from geopolitics, the EU increasingly needs to regard market access as an instrument of statecraft.[57]

The single currency provides another underused source of geopolitical influence. In 2025, the euro was used for 50.4% of EU manufactured-goods exports and 62.2% of primary-

[55] European Commission, *Cloud Sovereignty Framework: Implementation Guidance* (European Commission, 1 June 2026).

[56] European Commission, *DG Trade Statistical Guide* (European Commission, August 2026).

[57] See, e.g., Thomas Verellen, "Economic Security and the Transformation of EU Trade Policy," in Steven Blockmans and Panos Koutrakos (eds), *Research Handbook on the EU's Common Foreign and Security Policy* (Edward Elgar, 2027).

goods exports outside the EU.[58] The euro is no substitute for the US dollar, whose global financial role remains substantially greater. But the EU's monetary and financial infrastructure gives it leverage that should be integrated more deliberately into its geopolitical strategy.

Most importantly, the EU can build coalitions. By aggregating its values, market, capital, technology, standards, finance, and diplomacy into partnership packages, the EU can make cooperation with it more valuable than alignment with any single rival.

3.2. Turning Capacity to Act into Geopolitical Leverage

Given the EU's market size and suite of policy instruments, the strategic question is whether the EU can convert its economic and institutional weight into geopolitical leverage in a world where power is increasingly intangible, networked, and contested. That requires three changes.

- **First**, the EU needs better measures of power in the digital world. GDP and trade remain essential, but they should be supplemented by indicators of computing capacity, intellectual property, data assets, technological dependencies, critical infrastructure, semiconductor capabilities, financial connectivity, and control of standards.

- **Second**, the EU should identify which strategic chokepoints it owns. Others' dependencies on them – whether in advanced industrial equipment, pharmaceuticals, aerospace, standards, specialised manufacturing, or market access – are potential instruments of the EU's geopolitical influence.

- **Third**, the EU needs to use its economic instruments more strategically. The Commission's 2025 update of the European Economic Security Strategy already points towards a more assertive deployment of the EU toolbox, moving from reactive risk management towards anticipation, deterrence, and response.[59] The 2026 European Tech Sovereignty package represents a similar shift, targeting semiconductors, AI, cloud infrastructure, and open-source technologies.[60] The direction is correct, but policy announcements do not themselves create technological sovereignty.

Navigating between digital empires, the EU's most realistic course lies in being a geoeconomic power able to mobilise a sizeable Single Market, advanced industrial base, regulatory system, currency, and diplomatic network in pursuit of strategic objectives.[61] That requires a shift from measuring what the EU possesses to measuring what the EU can make others do.

The EU should be willing to pay a premium, intervene offensively, and accept some inefficiency where failure would threaten national security or political autonomy

The EU should be willing to pay a premium, intervene offensively, and accept some inefficiency where failure would threaten national security or political autonomy. Advanced chips, critical cloud infrastructure, military AI, secure communications, and key energy technologies fall into this category. In less strategic areas, the EU should remain open to global competition.

This approach would reduce the risk of 'sovereignty inflation', the tendency to label every technology strategically indispensable and consequently justify ever-greater intervention. Not every European software company needs protection; not every foreign acquisition threatens sovereignty; not every imported AI model represents strategic dependence. The test should be: Could losing access materially constrain the EU's ability to make independent political choices? If not, then the case for intervention is considerably weaker.

[58] "Euro dominates extra-EU trade in primary goods," Eurostat, 11 May 2026.

[59] European Commission, *Joint Communication to the European Parliament and the Council, 'Strengthening EU economic security'*, JOIN/2025/977 final (European Commission, 3 December 2025).

[60] European Commission, *European Tech Sovereignty*.

[61] Anu Bradford, *Digital Empires. The Global Battle to Regulate Technology* (Oxford University Press, 2023).

A realistic EU strategy would therefore identify domains where Europe can establish indispensable capabilities.

- **First**, industrial AI. As noted, Europe possesses world-leading automotive, aerospace, pharmaceutical, chemical, energy, and advanced-manufacturing industries. These sectors generate enormous quantities of specialised data and operational knowledge. The opportunity is to build AI systems deeply integrated into these industries rather than try to reproduce Silicon Valley's consumer-platform model.

- **Second**, open and interoperable AI. This could become a genuine European strategic niche. The EU's Open Source Strategy explicitly aims to reduce dependencies across the technology stack. The Union should distinguish between open models and merely available models. Genuine technological agency requires access to model weights where appropriate, reproducible infrastructure, transparent standards, European computing power, and the ability to fine-tune and deploy systems independently. This could allow the EU to create a third space between proprietary American AI and politically controlled Chinese AI.

- **Third**, trusted infrastructure. Europe can become a major provider of AI infrastructure where security, privacy, resilience, and democratic accountability are strategic requirements. This is particularly relevant for governments, healthcare, defence, energy, and critical infrastructure.

Europe can become a major provider of AI infrastructure where security, privacy, resilience, and democratic accountability are strategic requirements

- **Fourth**, semiconductors and advanced industrial technology. Europe is unlikely to become self-sufficient across the semiconductor chain. That is neither realistic nor necessary. But maintaining control over critical niches, particularly advanced equipment, specialised chips, materials, and industrial manufacturing, can provide disproportionate leverage.

3.3. Regulate Against the Machine?

As the AI industry expands and evolves with every passing week, so the campaign for AI regulation morphs with it.

Generally speaking, regulation can protect the public, but it can also create barriers to entry. Large firms with substantial sunk costs may be better able to absorb compliance expenses than smaller competitors. Rules designed around the business models of incumbent firms could therefore slow competition and reinforce concentration rather than improve safety.

AI regulation presents specific policy dilemmas. For instance, firms that benefit from broader adoption of open models may favour a different regulatory approach. Competition from Chinese models is a potential challenge to the economics of costly frontier systems.

A more challenging dilemma concerns whether existing legal constructs can mitigate or compensate for harm. Legal principles and tools, including negligence, product liability, and consumer protection, can address some harms but may be inadequate for risks that are probabilistic, difficult to attribute, irreversible, or potentially catastrophic. At the same time, calls for new regulation from leading AI companies may reflect genuine safety concerns, commercial efforts to slow competitors, or both. Effective governance requires not only rules, but also independent scrutiny, credible reporting requirements, and sufficient public-sector expertise to enforce them.

Tort liability, both in the common law and continental European traditions, offers a practical starting point for governing AI. Negligence, product liability, professional malpractice, nuisance, and various other concepts of contract law and consumer protection may provide remedies when AI systems cause foreseeable harm. The threat of liability – including actions for damages before the Court of Justice of the EU – can incentivise developers to test systems and prevent foreseeable harm before release.

However, liability is largely retrospective. It is a poor fit for damages that cannot be compensated after the fact, including major security crises or existential risks. Extremely large potential liabilities are difficult to estimate and price in, could be challenging for companies to absorb, and might ultimately shift some risk onto the state. Attribution may also be difficult when model behaviour is probabilistic and causal pathways are opaque. Effective oversight and enforcement depend on regulators learning when systems behave dangerously. If reporting an incident increases a company's legal exposure, firms may have incentives to underreport or frame incidents narrowly. A liability-based approach therefore needs reliable reporting, monitoring, and enforcement arrangements.[62]

Effective oversight requires expertise across machine learning, computing infrastructure, cybersecurity, biological risks, competition policy, and national security. The US has relevant expertise across agencies and research institutions, but it faces difficulties coordinating that expertise, keeping it current, and competing with private-sector salaries. Fragmentation in American AI governance is compounded by political uncertainty and disagreement over the strategic direction of AI development between institutions at the federal and state levels. This is a bad match for the EU's emerging governance framework. China provides a contrasting model: a more centralised system capable of enforcing red lines, particularly where AI threatens the Communist Party's control. Obviously, autocratic centralisation should not be confused with universal regulatory superiority.

The question is what combination of preventive oversight, transparency, competition safeguards, liability, and public-sector capacity can address the risks posed by frontier AI and RSI. A credible regulatory framework should be proportionate to risk, enforceable in practice, open to independent examination, and designed to protect the public without unnecessarily consolidating market power.

[62] On the shortcomings of the EU's current regulatory framework, see: Luise Quaritsch, "Beyond Dependency Enforcing EU Rules Against US Big Tech," *Hertie School Jacques Delors Centre*, 19 October 2026.

As an aside, one of the EU's least-used instruments may be its most powerful: joint procurement. The EU and its member states collectively represent enormous demand for cloud computing, cybersecurity, AI, software, telecommunications, energy technology, and defence systems. Procurement can therefore create markets for European companies without formally excluding foreign competitors. The Commission's cloud sovereignty framework already demonstrates this approach by incorporating sovereignty criteria into public-sector procurement. The principle could be expanded. Rather than asking whether a supplier is European, governments could score suppliers on resilience, jurisdictional exposure, interoperability, supply-chain concentration, data control, technological substitutability, and contribution to European strategic capability. This is more defensible economically and politically than crude 'buy European' rules.

One of the EU's least-used instruments may be its most powerful: joint procurement

3.4. A New Bargain

The emerging European policy model should therefore be neither laissez-faire nor protectionist. It should be based on a three-part bargain:

- **First**, the EU remains open to global technology and investment.
- **Second**, Europe builds domestic capabilities where dependence would create strategic vulnerability.

A Europe that regulates everything but cannot produce and scale technology will have limited geopolitical agency

- **Third**, the EU retains the ability to impose restrictions where foreign economic power threatens European security or political autonomy.

This requires regulatory restraint as much as regulatory ambition. That is strategically important. A Europe that regulates everything but cannot produce and scale technology will have limited geopolitical agency.

4. Trade-Offs

4.1. Resilience vs Competitiveness

A tougher posture has an obvious attraction. If European governments systematically favour secure European cloud, AI, and semiconductor suppliers, as the Commission's new tech sovereignty agenda advises, then they can create demand that helps European companies scale.

But sovereignty has a price. European companies may have to pay more for European or trusted infrastructure than for the cheapest global alternative. Restricting foreign suppliers can reduce competition. Localising supply chains can duplicate capacity. Data and technology requirements can impose compliance costs. Export controls can prevent European companies from selling into lucrative markets. This is particularly dangerous for the Single Market, already concerned about weak productivity and insufficient investment.

The EU's own competitiveness agenda recognises this tension. Its 2026 "One Europe, One Market" roadmap explicitly combines strategic autonomy with simplification, deeper integration, and lower administrative burdens, targeting €37.5 bn in annual savings from reduced costs by 2029.[63]

The EU cannot maximise protection, regulation, resilience, and affordability – it must decide where the sovereignty premium is justified

This is not an incidental detail. It points towards the essential bargain underpinning European digital sovereignty: the EU cannot simultaneously maximise protection, regulation, resilience, and affordability. It must decide where the premium for sovereignty is justified.

4.2. Unity vs National Interests

The EU faces another constraint: the interests of member states do not always coincide. France may favour strategic autonomy and European industrial policy. Germany may prioritise industrial competitiveness and access to global markets. Smaller member states may fear that protectionism will disadvantage them or reduce foreign investment. Countries with major technology sectors may resist policies that restrict relationships with American companies.

This creates a familiar European dilemma. The EU has far more bargaining power collectively than its member states possess individually. But the more politically sensitive the issue, the harder collective action becomes. A European cloud strategy, for example, is relatively straightforward when framed around cybersecurity and resilience. It becomes more contentious when it effectively excludes American suppliers. Similarly, supporting European semiconductor production is broadly uncontroversial. Imposing restrictions on foreign technology can produce much sharper political divisions.

The EU needs a 'Made in Europe' approach to AI regulation where the geographic reach of the impending Industrial Accelerator Act extends to third countries that are party to the WTO Government Procurement Agreement or have a Free Trade Agreement with the EU and that are willing to offer equivalent commitments and reciprocity.[64] A strategic approach would follow that pursued for Permanent Structured

[63] European Parliament, the Council of the European Union and the European Commission, *One Europe, One Market Roadmap* (European Commission, 24 April 2026).

[64] General Secretariat of the Council, *Regulation on accelerating industrial capacity and decarbonisation (Industrial Accelerator Act) - Guidance for further work*, Council doc. 13708/26 (General Secretariat of the Council, 30 September 2026). See: Lisa O'Carroll, "France drops opposition to UK being included in 'Made in Europe' legislation," *The Guardian*, 15 October 2026. In return, the UK government committed to align with the EU's position over tariffs on Chinese electric vehicles (EVs).

Cooperation (PESCO) in defence, where a Council decision establishes strict eligibility conditions for third-country participation that could be adapted to serve the EU's values and interests in the tech domain:

- **Political**: countries must share EU values, support Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP) objectives, and not harm EU security and defence interests;
- **Substantive**: countries must provide substantial added value, as well as technical, operational, or financial support, and not delay project progress;
- **Legal**: countries must have a Security of Information Agreement with the EU and an Administrative Arrangement with the European Defence Agency where applicable.[65]

4.3. The Transatlantic Trade-Off

The hardest political calculation concerns the United States. Europe's dependence on US technology is simultaneously a vulnerability and an asset. American companies provide access to technologies Europe cannot currently reproduce at equivalent scale. A confrontational EU policy could therefore harm European companies and consumers.[66]

The objective should be to develop sufficiently credible alternatives so that European policymakers have choices

Rather than (in)discriminately reducing the involvement of American tech companies, the objective should be to develop sufficiently credible alternatives so that European policymakers have choices. This is the aim of EU cloud, AI, and semiconductor investment.

By the same token, the EU should not relent on its own ethics code. The case of the DSA, which – like the DMA – specifically aims at very large online platforms and companies that act as gatekeepers, has seen Google, Apple, Meta, Amazon, and Microsoft fined more than €20 bn since the start of 2021.[67] The initial outcry from the tech companies and pushback from the White House may be a boon to more progressive forces at the state level seeking to follow the EU's regulatory lead (e.g., on child safety).[68] It may pave the way for acceptance by industry and the MAGA movement, especially if Chinese competitors are also targeted by investigations.

Paradoxically, European technological capability can thus strengthen the transatlantic relationship rather than weaken it. A partner with alternatives is more valuable, and more capable of negotiating, than a dependent customer.

4.4. China Creates a Different Trade-Off

The China question is more difficult because the economic and political dimensions are harder to separate. Chinese technology can contribute to competition and diversification. Open-weight AI models may offer European developers alternatives to proprietary American systems. Chinese manufacturing capabilities can reduce costs and provide supply-chain options. Yet strategic dependence on Chinese technology can create different vulnerabilities, particularly where technologies intersect with surveillance, censorship, data governance, or critical infrastructure.

Here too, the answer should not be blanket technological exclusion. Instead, the EU needs risk differentiation. The appropriate policy depends on what the technology

[65] Council Decision (CFSP) 2020/1639 of 5 November 2020 establishing the general conditions under which third States could exceptionally be invited to participate in individual PESCO projects, OJEU (2020) L 371/3. The PESCO project on military mobility includes the US, Canada, Norway, the UK, and Switzerland.

[66] Barbara Moens and Henry Foy, "US threatens European companies over Starlink restrictions," *The Financial Times*, 18 October 2026.

[67] Quaritsch, "Beyond Dependency."

[68] Rather dubiously, the US Federal Trade Commission, on 21 August 2025, issued a stern warning to major tech firms not to comply with the EU's DSA if it compromises American values like free speech or encryption integrity. See, e.g.: Hezekiah Ortiz, "Digital Sovereignty in Tension: U.S. Pushback Against the EU's Digital Services Act," *The Cyber Institute*, 31 August 2025.

does, what data it accesses, whether it can be independently audited, whether credible alternatives exist, and whether dependence could be exploited during a political crisis. This is where the EU's regulatory capacity can become a geopolitical asset.

The EU needs risk differentiation

Conclusion and Recommendations: Balancing Act

Europe is not trapped between the US and China. Its room for manoeuvre is narrower than that of either superpower, but considerably wider than self-deprecating talk about a 'digital colony' implies. The EU can regulate access to its market, shape standards, direct public procurement, support strategic industries, screen dependencies, coordinate member-state resources, and impose economic countermeasures. The 2026 tech sovereignty package shows that Brussels is increasingly attempting to integrate these instruments rather than treat digital policy, industrial policy, and economic security as separate domains.

The difficulty is political. A tougher European posture produces real costs: higher prices, reduced competition, potential retaliation, weaker foreign investment, and greater fragmentation of global technology markets. Excessive intervention could weaken precisely the economic base on which European power depends.

A realistic objective is maximum agency at acceptable cost. The EU should be tough where dependency threatens strategic freedom; open where competition benefits European consumers and firms; interventionist where public procurement can create scale; and continuously focused on reducing the dependencies that matter most.

The ultimate measure of European tech sovereignty could be formulated quite simply: when a major technology supplier threatens to withdraw access, change terms, or align with a geopolitical adversary, does the EU have credible alternatives? Where the answer is 'yes', the EU has agency. Where the answer is 'no', that is where European tech policy should focus next.

To achieve interdependence with agency, the EU needs to work towards a positive transatlantic technology agenda in which the US retains its enormous innovation and capital advantages, Europe contributes market scale, industrial capability, regulation, and investment, and both sides reduce their exposure to China without forcing each other into technological dependence.

That agenda is particularly urgent because the relationship is currently moving in the opposite direction. Washington is increasingly framing AI competition in bloc terms. Launched by the State Department as a strategic economic-security initiative, the Pax Silica focuses on securing AI infrastructure, semiconductor supply chains, and critical raw materials, while implicitly diluting China's dominance and coercive leverage in these sectors. The initiative unites more than 20 high-income and strategic partners, including the UK, Japan, and a growing list of Latin American nations such as Argentina and Chile. Through the Pax Silica, Washington is actively leveraging its dominance in advanced microchips, such as Nvidia hardware, and in cloud infrastructure. After some trepidation, notably from France, about the perceived threat to EU strategic autonomy, the European Commission, alongside Germany, Greece, and the Netherlands, officially signed a declaration, joining the coalition in June 2026.[69] The ink was barely dry when the State Department sent a letter to signatories in which it explicitly warned partner nations that they cannot participate in both the US framework and China's competing World AI Cooperation Organization (WAICO)

To achieve interdependence with agency, the EU needs to work towards a positive transatlantic technology agenda

[69] European Commission, "Commission signs Pax Silica declaration," 25 June 2026.

ecosystem.[70] At the same time, disputes between Washington and Brussels over EU digital regulation (in particular the DMA) and American tech companies are spilling into the wider trade relationship.[71]

A constructive transatlantic tech agenda has at least seven elements:

- conclude a transatlantic AI compact;
- pursue a transatlantic technology market, not a protectorate;
- jointly build the critical infrastructure neither side can afford to lose;
- create a transatlantic trusted-tech framework to blunt threats from China;
- develop a transatlantic AI and quantum research ecosystem;
- make European technological sovereignty compatible with American interests;
- establish a political bargain over regulation.

1. Conclude a transatlantic AI compact

The first priority should be to move beyond the traditional debate over AI regulation and establish a US–EU compact on AI capability. The objective would be to link American frontier-model and semiconductor capabilities with European industrial demand, research, and infrastructure. The EU–US Trade and Technology Council (TTC) should be revived in one form or another, imbued with a sense of purpose by being given a framework for cooperation on AI, 6G, and critical technologies.[72] The challenge is mainly political, but the machinery also needs to become more operational. A compact could establish cooperation on frontier AI research and safety; AI security and testing; shared research infrastructure; public-sector AI; scientific and medical applications; energy-efficient computing; AI cybersecurity; and common technical standards. Rather than joint regulation, the main objective would be joint capability-building, with both sides seeking interoperability where interests coincide.

2. Pursue a transatlantic technology market, not a protectorate

The US and EU should work towards a transatlantic market for trusted digital technologies. That means easier cross-border investment, interoperable standards, compatible cybersecurity requirements, and predictable rules for cloud, AI, and digital services. This must not become a euphemism for unrestricted access to the Single Market for American technology companies. Current disputes demonstrate that this will remain a contentious issue. Washington is pressing Brussels to modify aspects of its digital regulation, while the EU insists on its right to regulate its own market. The solution is regulatory dialogue with economic reciprocity. Where US and European rules achieve essentially the same objectives, the two sides should recognise one another's standards. Where they differ for legitimate political reasons, they should agree on mechanisms to manage the differences rather than turn every disagreement into a trade dispute.

3. Jointly build the critical infrastructure neither side can afford to lose

AI turns infrastructure into geopolitics. The transatlantic relationship should therefore focus heavily on semiconductors, data centres, cloud infrastructure, electricity grids, subsea cables, and telecommunications. This is particularly important because European weakness does not necessarily require the EU to duplicate the American tech ecosystem. Europe can build 'trusted redundancy': backup systems or data paths designed to be truly independent, verified, and secure.[73] The EU's 2026 decision to support seven AI gigafactories – with €10 bn in public funding intended to mobilise a further €20 bn in private investment – is an important step in that direction.[74] The US should see such

[70] Michael Martina, "US to tell partners they must pick sides in AI race with China," *Reuters,* 14 August 2026. On WAICO, see: Gerald Mako, "China's New AI Club: The World Artificial Intelligence Cooperation Organization," *The Diplomat*, 21 July 2026.

[71] Foo Yun See, "US lawmakers urge Trump to act against EU tech rules, suggest trade probes," *Reuters*, 21 June 2026. See also: Hans Kuepper, "AI Geopolitics Explained: EU AI Act vs US vs China," *PromptQuorum,* 26 August 2026.

[72] Aleksandra Wójtowicz, "Trade and Technology Council's Future in Question under Trump," *PISM*, 6 March 2025.

[73] See: NHI Mgmt Group Editorial Team, "What do teams get wrong about redundancy in infrastructure operations?," *NHI & AI Identity Journal*, 7 September 2026.

[74] European Commission, "EU launches AI Gigafactories call to boost Europe's computing capacity and unlock more than €30 billion in investment," 30 July 2026.

European investment as allied capacity. Washington should have an interest in an EU capable of providing trusted computing power, semiconductor equipment, industrial AI, and secure infrastructure rather than one permanently dependent on Chinese alternatives.

Europe can build 'trusted redundancy'

4. Create a transatlantic trusted-tech framework to blunt threats from China

This is where the relationship could become strategically transformative. The US is increasingly asking partners to choose sides. But a sustainable coalition cannot simply be based on using American rather than Chinese technology. The EU will resist that proposition, not only because of commercial interests but also because it wants technological agency. A better framework would establish common criteria for technologies considered trusted in strategic sectors. The test would not necessarily be nationality. It could include potential for political coercion; interoperability; control of sensitive data; cybersecurity; supply-chain transparency; ability to audit systems; and jurisdictional oversight. This would allow the US and Europe to establish a trusted technology space without requiring European governments to exclude every Chinese product from every market. It would also make the policy more defensible internationally.

5. Develop a transatlantic AI and quantum research ecosystem

There is a major opportunity to connect American capital and frontier laboratories with European scientific depth. AI should be obvious, but quantum may be even more promising because the competitive landscape remains unsettled. The EU and US have previously identified quantum as a priority within the transatlantic technology relationship.[75] The two sides could establish jointly funded programmes around quantum computing. The objective should be to create research networks that are difficult for geopolitical competitors to replicate, rather than merely sign another series of declarations.

6. Make European technological sovereignty compatible with American interests

This may be the most politically important element. Washington needs to understand that European tech sovereignty is not inherently anti-American. The EU's objective is to ensure that it has alternatives. American companies may ultimately benefit from this. A Europe capable of building its own computing, cloud, and AI capacity will be a stronger economic partner and a more capable security ally. The US should distinguish between European tech sovereignty that strengthens allied resilience and European protectionism that discriminates against American companies. The first should be encouraged; the second should be negotiated.

7. Establish a political bargain over regulation

Finally, both sides need to recognise that the regulatory dispute is not going away. The EU will continue to regulate technology more aggressively than the US. The US, meanwhile, is currently pursuing a considerably more deregulatory federal AI approach, while American states retain their own regulatory initiatives.[76] California, Colorado, New York, and Texas have emerged as the most active jurisdictions, enacting targeted legislation covering issues such as high-risk AI systems, transparency requirements, and chatbot disclosure obligations.[77] California, home to Silicon Valley and, were it an independent country, the world's fourth-largest economy, effectively forces national and global tech

Combining the Brussels and California effects would force a race to the top in global regulatory convergence

[75] European Commission, "EU-US Trade and Technology Council (2021-2024)," last modified 8 June 2026.

[76] Hope Anderson, Burak Haylamaz, and Alex Fields, "Who governs AI? The federal government's challenge to state regulation — What organizations need to know," *Reuters*, 12 August 2026.

[77] See: Gareth Skoes and Danny Tobey, "AI Laws of the World: United States," *DLA Piper*, 29 July 2026.

companies to adopt these high standards everywhere because it is too costly to maintain separate rules for just one state – the 'California effect'.[78] Where ideological differences prevent constructive cooperation at the federal level, the EU should establish diplomatic guardrails against regulatory conflict and at the same time seek alignment at the state level. Combining the Brussels and California effects would force a race to the top in global regulatory convergence.

By way of conclusion: neither the US nor the EU possesses everything required to compete with China across the entire technology stack. Together, they come considerably closer. But implementing a positive transatlantic tech agenda will only work if Washington accepts that European agency is an asset rather than a threat, while the EU accepts that strategic autonomy cannot mean technological exclusion of the US from the Single Market. The objective should be a course between dependency and decoupling: a strong transatlantic tech alliance in which the EU becomes sufficiently capable to be a genuine partner in building a more resilient ecosystem.

[78] Christal Hayes and Peter Hoskins, "California passes Japan as fourth largest economy," *BBC News*, 25 April 2025. See: Brooke Tanner, "Unlocking the California Effect: Insights from the Transatlantic Tech Exchange in Sacramento," *GMF*, 20 May 2024.

RECENT ICDS PUBLICATIONS

REPORTS

Gretskiy, Igor. ***Russian Expertise on Ukraine***. October 2026.

Hosaka, Sanshiro. ***Adapting to War: The Evolution of Russia's Intelligence Ecosystem***. September 2026.

Kohv, Marek; Henrik Praks, Shin Kawashima, and Keizo Kitagawa. ***Connecting the Ends: A Baltic–Indo-Pacific Agenda for Undersea Infrastructure Security***. July 2026.

Klyszcz, Ivan U.K., and Kristel Potsepp. ***Spinning the Globe: Russian Information Warfare and Its Reach into the Global South***. June 2026.

Klyszcz, Ivan U.K. ***Agents of Decolonisation? The Chechen and Circassian Diasporas in Europe since 2022***. May 2026.

Jermalavičius, Tomas (ed), Javad Keypour, François-Xavier Chevallerau, Koen Claessen, Kristel Potsepp, Henrik Praks, Emil Sondaj Hansen, Nolan Theisen, Izabela Surwillo, Tomas Janeliūnas. ***The Ties That Bind: Energy Connectivity in the Age of Geopolitical Turbulence***. April 2026.

Hanso, Toomas, Urmas Hõbepappel. ***Taiwani väina kriisistsenaariumid ja kriisi julgeolekumõjud Eestile***. March 2026.

Tynkkynen, Veli-Pekka. ***Draining Fuel from the Russian War Machine: Oil, Gas, and Sanctions Outlook***. March 2026

Hõbepappel, Urmas. ***The Yin and Yang of Russia's Image in China: Netizen Discourse and Real-Life Implications***. March 2026.

POLICY PAPERS

Eglit, Helena, Cattler, David. "**Trusted Autonomy in the AI Era: Safeguarding Democratic Decision Integrity**." July 2026

Brünner, Finn-Niklas. "**Shielding the Skies: European Ballistic Missile Defence**." December 2025.

Kallioniemi, Pekka. "**Beyond Defence: A Proactive Strategy for the West in the Information Domain**." November 2025.

ANALYSES

Fedosiuk, Tetiana. "**The Case for a Visa Ban: Pathways to Denying Russian (Ex-)Combatants Entry to the EU**." September 2026.

Breuer, Naomi. "**Fighting a War at Home: The Institutionalisation of Germany's Response to Russian Hybrid Attacks**." September 2026.

Giuashvili, Teona. "**Georgia's Foreign Policy Pivot**." July 2026.

Tomio, Giulio. "**Under the Russian Flag: Reflagging and the Future of Shadow Fleet Enforcement**." July 2026.

Hosaka, Sanshiro, and Elena Kim. "**Asia's Fallout from Russia's War Against Ukraine: North Korea's Rise in the Russia–China Balance**." April 2026.

Koizumi, Yu. "**The Bear's Sharp Claw or a Soft Underbelly? Russian Armed Forces in the Far East**." April 2026.

Akimenko, Valeriy, Keir Giles. "**The Russian Way of Ceasefires and the Traps It Sets for Europe**." March 2026.

BRIEFS

Lawrence, Tony (ed); Alessandro Marrone, Neeme Väli, Thierry Tardy, Justina Budginaitė-Froehly, Peter Viggo Jakobsen, Torben Schütz, Henrik Larsen, Andrea and Mauro Gilli, Armida van Rij. "**Europeanising NATO Series**." September 2026.

Fedosiuk, Tetiana. "**The Coalition for Ukrainian Children: Coordinating Commitments and Confronting Challenges**." September 2026.

Raik, Kristi (ed); Matti Pesu, Anders Wivel, Merili Arjakas, Helena Eglit, Margarita Šešelgytė. "**Small States Series**." August 2026.

Le Grand, Pauline; Hainaut, Béatrice. "**EU Defence Series**." July 2026.

Delval, Théa. "**The Special Tribunal for Ukraine: Turning the Wheels of International Justice.**" June 2026.

Delval, Théa, and Luca Rogers. "**Legality and Reality: The Eastern Flank and the Ottawa Convention Théa Delval Luca Rogers**." June 2026.

Rogers, Luca, and Felix Gasper. "**Germany's New Military Concept: Responsibility for Europe**." June 2026.

All ICDS publications are available from https://icds.ee/category/publications/.

ICDS.Tallinn
@ICDS-TALLINN.BSKY.SOCIAL
@ICDS _ Tallinn
ICDS _ Tallinn
www.icds.ee

International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee

ISSN 2228-2068