EPIS Thinktank
foreign affairs & security policy

Issue III
October 2026
epis-thinktank.com



EPIS REPORT on Artificial Intelligence & Cybersecurity



Route Sovereignty: The Missing Link in Europe's Digital Sovereignty Agenda

Why the cables carrying Europe's data belong at the heart of its digital sovereignty strategy

The Accountability Paradox of Commercial Spyware: the NSO Group Case

How Legal and Regulatory Failures Turned Pegasus' Spyware Into an Ungovernable Strategic Asset.

Table of Contents

Editorial

4 Editorial Team and Contributors

8 Editorial by Andrea Guidotti

Articles

9 **Route Sovereignty: The Missing Link in Europe's Digital Sovereignty Agenda**

Cliona Hennessy – Why the subsea cables carrying Europe's data belong at the heart of its digital sovereignty strategy.

19 **Sovereignty versus Autonomy: Europe's contradiction of Digital Dependency**

Silas van Gorkum – Has EU regulatory policy reduced Europe's foreign digital dependency – or only added more rules?

29 **AI Regulatory Divergence in Capitalist Regimes: A Comparative Analysis of the US, the EU and China.**

Esperança Bennassar Rivero – How varieties of capitalism shape AI regulation in the EU, the US and China.

39 **Economic Coordination and AI: Does AI Shift the Balance Between Markets and Planning?**

Fabian Wylczoch – Hayek's knowledge problem revisited: does artificial intelligence favour markets or planning?

Table of Contents

Articles

49 **Finland's Comprehensive Security Concept and its Strategic Applications for Stronger AI Readiness**

Sonja Liukkonen – How Finland's comprehensive security concept underpins its AI readiness against hybrid threats.

61 **Biometrics, Surveillance and Control at the Border.**

Laura Nicole Binetti – How the EU's Entry/Exit System tests Schengen's promise of free movement and the EU's AI rules.

71 **The Accountability Paradox of Commercial Spyware: the NSO Group Case**

Giulia Rossi – How legal and regulatory failures turned the Pegasus spyware into an ungovernable strategic asset.

Also Inside

18 **EPIS Newsletter**

Recent publications, awards and accomplishments of our Think Tank – continued in the FASP Newsletter on page 28. How to join EPIS: page 70.

Editorial Team



Editor / Report Group Leader

Andrea Guidotti holds an M.A. in World Politics and International Relations and a B.A. in Contemporary History and Philosophy. He has experience in policy and public opinion analysis, project management, market research, and AI training. His research focuses on the socio-economic and political impact of crises and technology, European integration, and populism. He currently serves as analyst at Trilations. Previously, he served as academic assistant at ITC-ILO and as research intern at ECPS.



Editor / Resort Leader

Sydney Armor leads the Thematic Report Groups of the EPIS Think Tank for Foreign Affairs & Security Policy. She holds a B.A. in International and Global Security Studies from Middlebury College and is a Fulbright Austria alumna: during her grant she taught English-language social and political topics at secondary schools in Graz and interned at Caritas on projects addressing gender-based violence. Based in Graz, she works as a Clinical Trial Associate, navigating international regulatory frameworks for global clinical trials.



Layout / Design Affairs

Abdullah Chaudhary is a Top Rated data engineer who builds industrial-grade web scraping, ETL pipelines, and automation systems that scale to millions of records. Over 3+ years, he has delivered 300+ custom solutions for startups and enterprises, maintaining a 100% Job Success Score.

& Contributors



Cliona Hennessy
Research Fellow



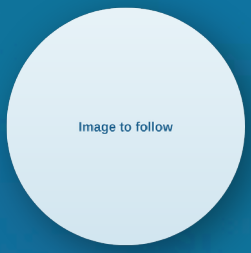
Silas van Gorkum
Research Fellow



Esperança Bennassar Rivero
Research Fellow



Fabian Wylczoch
Research Fellow



Sonja Liukkonen
Research Fellow



Laura Nicole Binetti
Research Fellow

& Contributors



Giulia Rossi
Research Fellow

Join EPIS

EPIS is both a network and a think tank in foreign and security policy. The EPIS Network connects students and graduates, supporting their careers. The EPIS Think Tank produces publications in various formats on different regions and topics. Together, they form EPIS—where you can join passively as a network member or actively contribute to publications. Interested? Apply now for an onboarding meeting & follow us on social media!

Want to author the next EPIS Report?

Apply for FASP now and contribute to one of our Report Groups – from Geographic Report Groups such as Europe to Thematic Report Groups such as Artificial Intelligence & Cybersecurity, Security Policy & Defence or Climate Policy & Environment.

epis-thinktank.com

Contact: board.external@epis-thinktank.com

Editorial



Report Group Leader, Artificial Intelligence & Cybersecurity

Andrea Guidotti holds an M.A. in World Politics and International Relations and a B.A. in Contemporary History and Philosophy. He has experience in policy and public opinion analysis, project management, market research, and AI training. His research focuses on the socio-economic and political impact of crises and technology, European integration, and populism. He currently serves as analyst at Trilations. Previously, he served as academic assistant at ITC-ILO and as research intern at ECPS.

EPIS Report on Artificial Intelligence & Cybersecurity

Dear reader,

Europe has spent two decades writing the rules of the digital age. It has done far less to build the capacities that would let it live by them. This third issue of the EPIS Report on Artificial Intelligence & Cybersecurity asks what digital sovereignty means in practice – beneath the sea, in our economies, at our borders and in the courtroom.

We begin with the infrastructure that is easiest to forget. Cliona Hennessy argues that Europe's sovereignty agenda has overlooked the subsea cables that carry its data, and introduces the idea of Route Sovereignty: the capacity to understand, protect, diversify and restore those routes. Silas van Gorkum examines the gap between the EU's regulatory sovereignty and its operational autonomy, and asks whether the Tech Sovereignty Package will build capacity or simply add more rules.

Two contributions look at how political economy shapes artificial intelligence – and how AI may reshape political economy in turn. Esperança Bennassar Rivero compares AI regulation in the EU, the US and China through the lens of Varieties of Capitalism and shows where strategic interests pull each case away from its model. Fabian Wylczoch revisits Hayek's knowledge problem and concludes that AI gives no general advantage to markets or to planning; its effect depends on the problem it is asked to solve.

The final three articles turn to security and rights. Sonja Liukkonen shows how Finland's comprehensive security concept, shared by authorities, business and citizens, has become the basis for strong AI readiness in defence and resilience. Laura Nicole Binetti assesses the EU's new Entry/Exit System and the risk of function creep in biometric border control. Giulia Rossi closes the issue with the case of the NSO Group and asks why commercial spyware has so far escaped accountability.

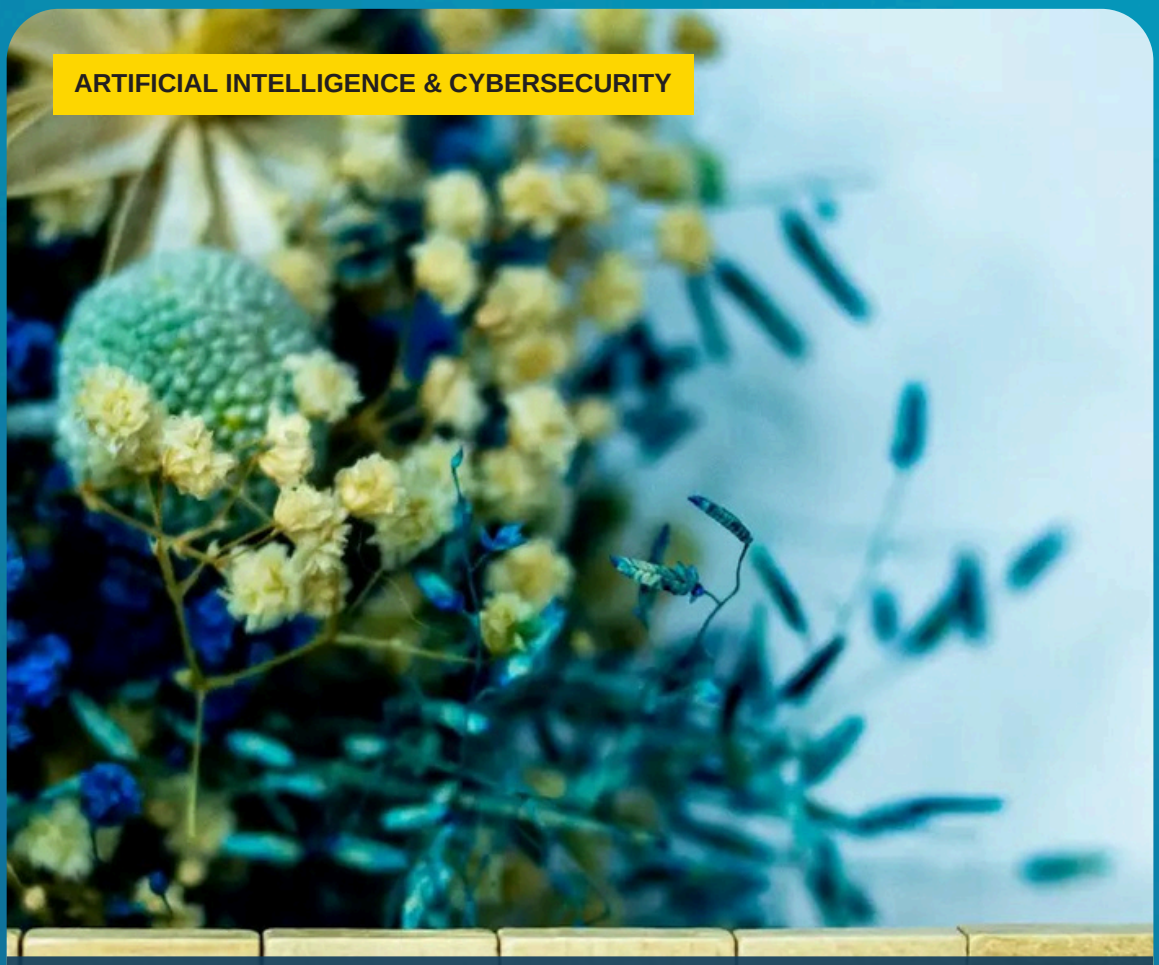
Taken together, the articles show that sovereignty in the digital age is not a matter of regulation alone. It depends on infrastructure, institutions and industrial capacity – and on the willingness to hold powerful technologies, and those who deploy them, to the standards we set.

I would like to thank all authors of the Artificial Intelligence & Cybersecurity Report Group for their work, and Sydney Armor and the Design Affairs team for making this issue possible.

I hope you enjoy reading it.

Andrea Guidotti
Report Group Leader, Artificial Intelligence & Cybersecurity

ARTIFICIAL INTELLIGENCE & CYBERSECURITY



Route Sovereignty: The Missing Link in Europe's Digital Sovereignty Agenda

Cliona Hennessy

About the Article

"The strategic problem, therefore, is not simply whether a cable breaks, but why it broke and whether that cause can be established with confidence."

About the Author

Cliona Hennessy is an Irish MSc student in Law, Economics and Governance in Bologna, following a BLB in Law & Business. Through her work at EUAbout, she gained experience across digital regulation, sustainability and trade. She is keen to explore a wide range of European affairs and build a career in informed, impactful EU policy.

Introduction

To many of us, the internet feels almost ethereal, an invisible current pulled from thin air, carrying information instantaneously from one screen to the next. But the data generated by our digital lives does not simply float around some nebulous cloud in the sky; much of it races beneath our feet through fibre-optic cables laid across the ocean floor. More than 400 of these cables, some no wider than a garden hose, span a combined 1.2 million kilometres across the world's oceans. Yet while Europe has built an extensive regulatory framework governing the data these cables carry, its approach to securing the routes they run along remains far less developed. This article calls this disparity Europe's 'Route Sovereignty' gap: the absence of an integrated EU approach to controlling and protecting the infrastructure through which European data moves between jurisdictions.

This does not mean the EU lacks cable regulation entirely. The NIS2 Directive (European Parliament & Council of the European Union, 2022a) and the Critical Entities Resilience (CER) Directive (European Parliament & Council of the European Union, 2022b) address some aspects of cable security, such as cybersecurity risk management, physical protection measures and incident reporting. The difficulty, rather, is that cable security remains dispersed across different regulatory frameworks and insufficiently integrated into the EU's wider digital sovereignty strategy. Now, as AI-enabled systems and autonomous technologies threaten to make undersea infrastructure easier to disrupt and responsibility for that disruption harder to trace, this gap is becoming increasingly difficult for Europe to ignore.

Why subsea cables matter

There is no overstating how much Europe depends on subsea cables. They carry over 99% of its intercontinental data traffic (International Telecommunication Union [ITU], 2026), leaving satellites to handle only a small remainder. But vulnerability is not simply a question of volume; it is also a question of location. Cables often cluster along the same transit corridors and share landing points, creating chokepoints where one disruption can affect several connections at once (European Union Agency for Cybersecurity [ENISA], 2023). Nowhere is this concentration more visible than in the Baltic Sea, where shallow, heavily trafficked waters host numerous telecommunications and energy links within a relatively small area. However, a broken cable is not always evidence of an attack. Anchoring and fishing account for nearly 40% of recorded faults, with human activity accounting for 87% of all incidents (ENISA, 2023). Nor does every break produce a crisis: built-in redundancy usually allows traffic to be rerouted when a single link fails. The strategic problem, therefore, is not simply whether a cable breaks, but why it broke and whether that cause can be established with confidence.

Recent incidents in the Baltic have brought this uncertainty into sharper focus. Between November 2023 and January 2025, four separate incidents saw telecommunications cables, power links and pipelines damaged by vessels operating in the region, repeatedly raising the same question: accident or deliberate interference? In a January 2026 report, the EU's Submarine Cable Infrastructures Expert Group

acknowledged that distinguishing accidental from intentional damage is "not always easy" (Submarine Cable Infrastructures Expert Group, 2026). Advances in autonomous underwater technology now add another layer to this uncertainty. Rossiter (2025) notes that roughly two-thirds of global seabed infrastructure lies within the three-kilometre diving range already achievable by uncrewed vehicles. Greater technological reach, however, does not automatically make cables more vulnerable: Rossiter also observes that increasing autonomy can benefit defenders as well as attackers. The technology is therefore changing both how subsea links can be threatened and how they can be protected. Against this evolving landscape, the fundamental question is whether Europe's governance of the infrastructure beneath its digital economy has kept pace with its strategic importance.

Route Sovereignty is the capacity to understand, protect, diversify and restore the physical routes, subsea cables, through which data moves.

The Missing Link in Europe's Digital Sovereignty

Europe's approach to digital sovereignty is extensive. The GDPR governs how personal data is processed and transferred, while recent initiatives have expanded the EU's focus to cloud services, AI, semiconductors and computing capacity. But the physical routes connecting these systems remain far less prominent. Nowhere is this disparity more apparent than in the Commission's 2026 Tech Sovereignty Communication, which commits €120 billion to semiconductors, €200 billion to data centres and €100 billion to cloud and AI leadership (European Commission, 2026b), while making no mention of subsea cable infrastructure as either an investment priority or a resilience concern. Europe's sovereignty ambitions extend deep into the technologies that store and process data, but far less comprehensively to the physical routes carrying it.

This reflects what Carrapico and Farrand (2025) describe as an "autonomy–interdependence gap" between Europe's digital ambitions and its reliance on infrastructure it does not fully control. Rudolph (2026) conceptualises digital sovereignty through three dimensions: data control, legal jurisdiction and vendor nationality. Route Sovereignty adds a crucial physical dimension by asking who protects the infrastructure carrying European data, how easily traffic can be rerouted during a disruption, and how much strategic influence Europe retains over those routes. Put simply, digital control is incomplete without comparable attention to the physical networks carrying the data.

Europe is beginning to address this blind spot. The Commission's 2025 Cable Action Plan (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2025) and Expert Group build on NIS2 and CER, bringing cables onto the digital policy agenda. The challenge is integration. ENISA, the European Fisheries Control Agency and the European Maritime Safety Agency, alongside Commission directorates DG CNECT, DG MOVE and DG MARE, hold partial mandates, while jurisdiction beyond national waters becomes less clear (ENISA, 2023). Private ownership adds

another tension. TeleGeography estimates over $14 billion in cable construction by 2027, driven largely by Big Tech (TeleGeography, 2025–2026). This gives private companies considerable influence over where critical routes are built and how they are operated, while governments remain responsible for protecting them and responding when disruption is suspected to be deliberate. Investment may be private, but security, investigation and defence ultimately require public authority. The Route Sovereignty gap is therefore not an absence of regulation or investment, but incomplete integration between private control of infrastructure, public responsibility for its security and Europe's wider ambitions for digital autonomy.

"The real test for Route Sovereignty is whether Europe can turn a warning into credible attribution, and credible attribution into a coordinated response."

Ireland: The Route Sovereignty Gap in Practice

Ireland offers a clear empirical test of the Route Sovereignty gap. As an island with no terrestrial alternative to subsea connectivity, its dependence on cables makes the tension between national capability, private ownership and EU resilience particularly visible. Fourteen cables connect Ireland internationally, including four transatlantic links and eight to the UK, but no dedicated telecommunications cable yet provides a direct operational route to mainland Europe (Submarine Cable Infrastructures Expert Group, 2026). For traffic between Ireland and continental Europe, this has meant heavy reliance on routes transiting the UK, which is now outside the EU's legal and security framework.

That dependence is particularly striking given Ireland's role in Europe's digital economy. Its 2019 National Cyber Security Strategy estimated that the country hosted over 30% of EU data (Department of Communications, Climate Action and Environment, 2019), although that figure should be taken with a pinch of salt as it predates the current AI-driven data-centre boom. A serious disruption to UK-linked routes would not necessarily disconnect Ireland, because built-in redundancy allows traffic to be rerouted. However, it would reduce the routes available between a major European data hub and the rest of the Union. Ireland's vulnerability therefore lies not simply in being an island. The deeper problem is that its strategic importance to Europe's digital economy has outpaced the diversity of its connections to mainland Europe.

National protection capacity compounds this problem. The Irish Naval Service operates eight vessels, but limited personnel means only around half are typically active, and none carries sonar capable of detecting activity below the surface (McCabe & Flynn, 2024). Ireland has begun to respond. Its 2026 National Maritime Security Strategy prioritises undersea infrastructure, while amendments to the Defence Act 1954 empower the Naval Service to board and redirect vessels threatening critical infrastructure (Department of Defence, 2026a, 2026b). EU policy is beginning to address the connectivity gap as well. The Cable Projects of European Interest (CPEI) framework proposes a direct Ireland–France–Iberia route to increase route diversity (Submarine Cable Infrastructures

Expert Group, 2026). Ireland therefore captures the Route Sovereignty gap particularly clearly. Despite its strategic importance to Europe's digital economy, it remains reliant on concentrated connectivity, constrained national protection and still-developing European coordination.

Accident or Attack? How AI Changes the Threat

Ireland's vulnerability, as the previous section shows, stems from concentrated routes, limited national capacity and coordination that is still catching up. But vulnerability alone does not tell us how great the threat really is. How likely is deliberate interference, and when a cable is damaged, can Europe reliably distinguish an accident from an attack? Most cable damage remains accidental, but that prevalence also creates cover for deliberate interference that can initially resemble a routine maritime incident. Under the UN Convention on the Law of the Sea (UNCLOS), coastal states can rarely act against a foreign vessel in international waters without cooperation from the country where it is registered, with cooperation often slow or withheld (Tammikko, 2025). Uncertain intent and limited enforcement therefore allow seemingly accidental conduct, such as anchor-dragging, to become a deniable means of interference. Redundancy may limit the immediate disruption, but Tammikko (2025) argues that it does little to identify or deter whoever caused it.

It is this difficulty in establishing intent that makes advances in autonomous technology increasingly significant. Rossiter (2025) argues that autonomy currently favours attackers because applications such as mine-laying drones and robotic cable-cutting arms remain simpler and cheaper to deploy than the sensing and repair systems needed to defend against them. Russia's 2022 Maritime Doctrine identifies underwater infrastructure as a potential target of state action (Loik, 2024). The Argus-D, an autonomous underwater vehicle developed by Russia's Rubin Design Bureau, illustrates the emerging capability. With the ability to operate at considerable depth and carry a 300-kilogram payload, it has what Sutton (2026) describes as "clear" offensive potential. But technological capability should not be mistaken for evidence of attack. No AI-enabled manipulation of vessel-tracking signals (AIS) or precision anchor-dragging has yet been documented against a European cable.

AI therefore changes the threat in a more subtle way. There is no evidence that it is already driving attacks on European cables. Instead, autonomous systems could make deniable interference cheaper and easier while making responsibility harder to establish. AI exacerbates an existing problem of attribution rather than creating an entirely new threat. For Route Sovereignty, protecting the route increasingly means being able to establish what happened along it.

AI as Defence, Not Just Threat

AI may complicate the question of who damaged a cable, but it can also provide new ways of finding the answer, strengthening the monitoring and detection capabilities Europe needs to spot suspicious activity before it escalates into full disruption. Rossiter (2025) frames this as a dual-use dynamic: the same autonomous technologies that may lower barriers to interference can also strengthen surveillance and detection. SEAuAIS, a self-explainable AI

model built on vessel-tracking (AIS) data, demonstrates this (Skat-Rørdam et al., 2025). Tested against vessel behaviour surrounding the 2022 Svalbard cable breach, it detected 15 of 16 known instances of suspicious behaviour, showing how AI can sift through volumes of maritime traffic that would be difficult to monitor manually. But its capabilities should not be overstated. Only 21% of its warnings identified genuinely unusual activity, meaning roughly four out of five were false alarms. AI can flag suspicious behaviour, but cannot determine whether it is accidental or deliberately hostile.

Detection is also moving beneath the waterline. The Submarine Cable Infrastructures Expert Group (2026) identifies Optical Fibre Sensing, particularly Distributed Acoustic Sensing and SMART (Science Monitoring And Reliable Telecommunications) cables, as technologies that could turn cables themselves into seabed sensors, detecting vibrations along their length rather than relying solely on vessels or satellites. VIGIMARE's pilot with Cinia already uses changes in light travelling through operational fibre to detect disturbances, with further trials planned for the Baltic, Mediterranean and Irish Sea from 2026. These technologies remain at an early stage, but point towards cables that could eventually help detect threats to themselves.

Better detection, however, is not the same as better protection. NATO's Critical Undersea Infrastructure Coordination Cell and Maritime Centre within Allied Maritime Command (MARCOM) connect naval surveillance with civilian operators, helping turn warnings into coordinated action. AI may therefore help narrow the attribution problem identified above, but it cannot resolve the legal and institutional barriers to acting on that information. The real test for Route Sovereignty is whether Europe can turn a warning into credible attribution, and credible attribution into a coordinated response.

From Data Sovereignty to Route Sovereignty

The limits of AI-based detection point to a wider lesson. Better technology cannot secure Europe's subsea infrastructure if the institutions responsible for acting on that information remain fragmented. The same problem runs through the Route Sovereignty gap more broadly. Control over data, regulation, computing capacity and suppliers cannot guarantee digital resilience if the physical infrastructure connecting those systems remains unevenly protected across institutions and countries. Digital sovereignty cannot stop at the data; it must extend to the routes that make its movement possible.

Europe is increasingly recognising this connection. Since 2024, the Commission's Recommendation on submarine cable infrastructures (European Commission, 2024), the Cable Action Plan (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2025), and the Expert Group's reports and Toolbox (Submarine Cable Infrastructures Expert Group, 2025, 2026) have given cable security greater institutional weight, while CPEI funding is beginning to translate policy into investment. Cable governance has therefore moved from relative obscurity to active, if still fragmented, EU attention. The Route Sovereignty gap is not static. It is better understood as incomplete and developing rather than absent.

Closing it requires bringing subsea connectivity into the EU's wider conception of digital sovereignty and directing investment towards the vulnerabilities identified throughout this article, including alternative routes, faster repair capacity and greater geographic diversity. This does not necessarily require another institution. The Expert Group's Toolbox already recommends a single coordinating entity in each Member State for cable security and resilience, closely mirroring the solution proposed for Ireland through MARA. Ireland's coordination problem is therefore not uniquely Irish, but one expression of a wider European challenge. Better monitoring and investigation are equally important. AI may help identify suspicious behaviour, but cannot overcome the legal and institutional barriers to establishing responsibility.

Ireland remains a sharp test of whether these commitments translate into resilience on the ground. Absolute control over every cable is neither realistic nor necessary. What matters is Europe's capacity to understand, protect, diversify and restore the routes on which it depends, and to coordinate responsibility when disruption occurs. Route Sovereignty therefore extends digital sovereignty beyond control of the data to resilience of the physical networks that carry it.

Conclusion

Europe's digital sovereignty ultimately rests on something far more physical than the term suggests. The cables beneath its surrounding seas carry the data on which its digital economy depends, but their security has not developed with the same coherence as the rules governing that data. The Route Sovereignty gap is therefore real, although it is a gap of fragmentation rather than neglect. Ireland makes the consequences particularly visible, with a major EU data hub still heavily dependent on routes through a non-EU state while national protection capabilities and European coordination continue to develop. AI adds another layer to this challenge, potentially making interference harder to trace while also offering new tools to detect it. Technology alone, however, cannot substitute for resilient routes, clear responsibility and coordinated action.

Europe does not need to control every cable beneath the sea to claim digital sovereignty. What it does need is the capacity to understand where its critical routes run, protect and diversify them, establish responsibility when disruption occurs and restore connectivity quickly. The EU has begun moving in that direction, but Route Sovereignty remains incomplete. Europe has spent years strengthening sovereignty over its data. The next challenge lies beneath it.

References

Bandura, R. (2025). The strategic future of subsea cables: Ireland case study. Center for Strategic and International Studies.

Bhalla, A. (2026). Europe must address the digital sovereignty triad. Atlantic Council.

Brown, E. (2025). The Baltic Sea at a boil: Connecting the shadow fleet and episodes of subsea infrastructure sabotage. Carnegie Endowment for International Peace.

Bueger, C. (2025). The hidden maritime frontier of artificial intelligence.

Carrapico, H., & Farrand, B. (2025). EU data sovereignty: An autonomy–interdependence governance gap? Politics and Governance, 13, Article 10331.

Davenport, T. (2015). Submarine cables, cybersecurity and international law: An intersectional analysis.

Department of Communications, Climate Action and Environment. (2019). National cyber security strategy 2019–2024. Government of Ireland.

Department of Defence. (2026a, February). National maritime security strategy 2026–2030. Government of Ireland.

Department of Defence. (2026b, March). New legal powers for Naval Service [Press release]. Government of Ireland.

Edwards, C., & Seidenstein, N. (2025). The scale of Russian sabotage operations against Europe's critical infrastructure. International Institute for Strategic Studies.

European Centre for Development Policy Management. (2026). Troubled waters: Europe's subsea telecommunications network (Briefing Note No. 208).

European Commission. (2024, February 26). Commission Recommendation on secure and resilient submarine cable infrastructures.

European Commission. (2026a, June). CEF-Digital second call for proposals to increase Europe's submarine cable repair capacities.

European Commission. (2026b, June 3). 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.

European Commission. (2026c). Guarding Europe's hidden lifelines: How AI could protect subsea infrastructure. Horizon Magazine.

European Commission. (2026d, February 5). Submarine cable repair capacities.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2025, February 21). EU action plan on cable security [Joint communication].

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2026, March). Joint communication to strengthen the security and resilience of submarine cables.

European Parliament & Council of the European Union. (2022a). Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333.

European Parliament & Council of the European Union. (2022b). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities (CER Directive). Official Journal of the European Union, L 333.

European Union Agency for Cybersecurity. (2023). Undersea cables: What is at stake?

Finnish Security and Intelligence Service. (2026). National security overview 2026.

Institute of International and European Affairs & Vodafone. (2026). Secure connections: Ireland's digital infrastructure and the resilience of European connectivity.

International Telecommunication Union. (2026). International Advisory Body on Submarine Cable Resilience: Report of the working groups 2026.

Jones, B. D. (2026, February 13). Seabed zero: Baltic sabotage and the global risks to undersea infrastructure. Bulletin of the Atomic Scientists.

Loik, R. (2024). Undersea hybrid threats in strategic competition. Journal on Baltic Security.

McCabe, R., & Flynn, B. (2024). Under the radar: Ireland, maritime security capacity, and the governance of subsea infrastructure. European Security.

Mok, C. (2026). Toward undersea cable resilience: The case for global collaboration. Texas National Security Review.

Rossiter, A. (2025). Cable risk and resilience in the age of uncrewed undersea vehicles (UUVs). Marine Policy, 171, Article 106434.

Skat-Rørdam, H. V., Kjærsgaard, R. D., Hovad, E., & Clemmensen, L. K. H. (2025). SEAuAIS: A self-explainable autoencoder with AIS-based maritime anomaly detection. Ocean Engineering, 341, Article 122656.

Submarine Cable Infrastructures Expert Group. (2025). Security and resilience of EU submarine cable infrastructures. European Commission.

Submarine Cable Infrastructures Expert Group. (2026, January). Submarine cable security toolbox and Cable Projects of European Interest. European Commission.

Sutton, H. I. (2026, January 2). Russian XLUUV concept: Argus-D. Covert Shores.

Tammikko, T. (2025). The EU and NATO in pursuit of better deterrence: Baltic Sea sabotage prompts rethink of current practices (Briefing Paper 02/2025). Finnish Institute of International Affairs.

TeleGeography. (2025–2026). Global bandwidth research service: State of the network.

UK Parliament, Joint Committee on the National Security Strategy. (2025a). Subsea telecommunications cables: Resilience and crisis preparedness.

UK Parliament, Joint Committee on the National Security Strategy. (2025b, December 18). Subsea telecommunications cables: Resilience and crisis preparedness: Government response.

Wall, C., & Morcos, P. (2021). Invisible and vital: Undersea cables and transatlantic security. Center for Strategic and International Studies.

Windward. (2026). Q2 2026 undersea cables risk report.

October 2026

EPIS

The EPIS Newsletter brings together the latest insights and publications from our Thinktanks, the EPIS Network, and EPIS Consult.
Stay engaged and join the conversation!

@episthinktank epis-thinktank.com
EPIS Thinkthank @EPISThinkTank

This Month at a Glance:

- **EPIS Launches EPIS News, Covering Daily Political News Across Different Countries**
- **EPIS Introduces the Alpha Version of its Internship Platfor**

Fellow of the Month



Our FASP Leader **Dmytro Sochnyev** is your Fellow of the Month in September! Dmytro he keeps our schedule organised and ensures smooth FASP operations, and thereby ultimately helps your publications shine. Thank you for your work Dmytro, we are looking forward to the next hills we will climb!

Board of Directors



We are currently expanding our ILCJ branch. A warm welcome to **Cem Sunay** as Thematic Working Groups Leader, **Carmen Ghetu** as ILCJ Blog leader, all leaders of the individual thematic report and working groups, and all new ILCJ fellows!

Board of Advisors



Viola von Cramon-Taubadel is a German politician from Alliance 90/The Greens. She served in the Bundestag and European Parliament, working on foreign affairs, EU-Russia relations, and EU-Ukraine relations.

Interested in learning more about our board of advisors and in contributing to our work?
Become a Think Tank Fellow Now!

Viewer Stats

▲ 49,400 (+52.0%)	▲ 15,093 (+1.5%)
▲ 58,280 (+27.8%)	▲ 4,274 (+23.8%)

EPIS Track Record

Journal Database
Accesible insights at your fingertips

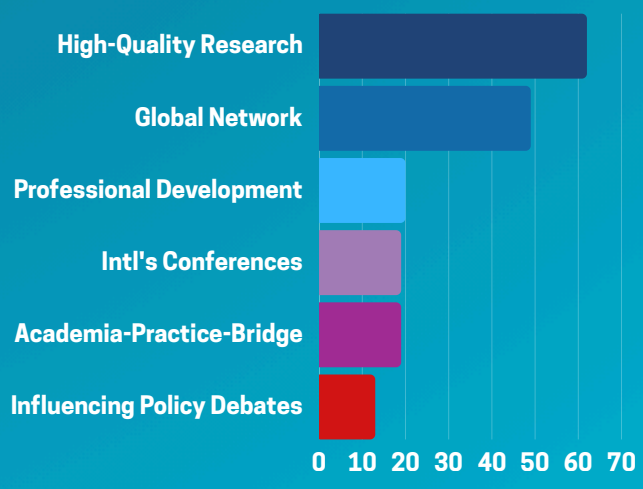


Monthly EPIS Awards
Your publications deserve recognition - every month



Question of the Month

What should EPIS be known for in five years?



ARTIFICIAL INTELLIGENCE & CYBERSECURITY



Sovereignty versus Autonomy: Europe's contradiction of Digital Dependency

Silas van Gorkum

About the Article

"A Microsoft server in Amsterdam puts Europeans at the risk of American law."

About the Author

Silas is a recent International Relations graduate currently working in public affairs. His academic and professional interests focus on Eurasia, Europe, and North America, with a particular emphasis on international economics, AI policy, and security and defense. Through EPIS's working groups, he aims to deepen his research experience in these areas while contributing to analytical projects and publications.

Introduction

In 2026 the European Commission presented the Tech Sovereignty Package, the latest instrument in a regulatory sequence running from the GDPR (General Data Protection Regulation), NIS2 and the Cybersecurity Act. This continues an unresolved contradiction. The EU has spent two decades building the world's most demanding cybersecurity rulebook, yet Europe is still dependent on foreign providers.

Two forms of sovereignty separate here. Regulatory sovereignty is the authority to set enforceable rules within a jurisdiction. Operational autonomy is the capacity to keep functioning without a foreign power's cooperation. Edler et al. (2023) define technology sovereignty as the capacity to act, and this article adopts their definition as its single test. The EU advanced on the first while the second stalled.

The contradiction frames the following question: to what extent has regulatory sovereignty over digital infrastructure produced the operational autonomy member states need to exit non-European providers, and which policies widen their ability to do so? Three measures structure the answer: legal exposure to foreign compulsion, supply continuity, and time.

The Scale of Dependency

The European Commission's own numbers are in evidence. The explanatory memorandum for the 2026 Cloud and AI Development Act (CADA) states the collective cloud market share of EU-based providers fell from roughly 29 per cent to about 15 per cent in 2022 (Gundermann, 2026); three US hyperscalers now hold more than 70 per cent of the market (van Klinken, 2026). According to a European Parliament report, digital products, services and infrastructure from non-EU sources are over 80 per cent (Khafo, 2025).

No European hyperscaler matched US providers in price or scope, and years of "Cloud First" procurement that followed defaulted to the platform was already inside the government IT department. A legal mechanism turns this commercial choice into a jurisdictional one. The US CLOUD Act mandates that American firms provide data to US authorities at any time (Cross-Border Data Sharing under the CLOUD Act, 2025). A Microsoft server in Amsterdam puts Europeans at the risk of American law.

Regulatory Autonomy is the capacity of a government or institution to independently plan for and conduct operations without relying on an external power.

Anton Carniaux of Microsoft France testified on 10 June 2025 to a French Senate committee on public procurement and digital sovereignty. When he was asked to guarantee French citizens' data would never reach US authorities without French government consent, he answered under oath: "No, I cannot guarantee it" (CE Commande Publique: Compte Rendu De La Semaine dU 9 Juin 2025, 2025). Microsoft's technical director for the French public sector, Pierre Lagarde, told the same hearing that customer data had been within the EU since a

contract in January 2025 (CE Commande Publique: Compte Rendu De La Semaine dU 9 Juin 2025, 2025). Both statements are true, but there is no legal guarantee in a technical arrangement.

Cases of Digital Exposure

The two cases in EU jurisdiction further illustrate the problem: EU law found the digital arrangements unlawful, and resolution still took years.

France centralised the health records of millions of citizens on Microsoft Azure because officials judged no European provider matched the scale (Marchandon, 2026). The 2020 Schrems II ruling struck down the transatlantic Privacy Shield, and France's data protection authority told the Conseil d'État Microsoft's safeguards were deficient, and the hosting was illegal (McDermott Will & Emery, 2020). The court allowed supervised continuation. The government promised to migrate to a European facility by the end of 2022, and the deadline slipped for years. The Hub moved to Scaleway, a French company, in April 2026 (Marchandon, 2026). Regulation flagged the problem in 2020. Six years passed before a change of provider resolved the problem, and capacity constraints caused the delay.

In November 2022, Germany's federal and state data protection authorities concluded public bodies had no path to compliant use of Microsoft 365 under EU data law without additional safeguards (Lomas, 2022). The European Data Protection Supervisor found in 2024 that the Commission's own use of the software breached EU data protection rules (European Data Protection Supervisor (EDPS), 2024). Microsoft provided the fix. EU Data Boundary build-out was completed in February 2025, Data Protection Addendum was made public in September, and the German state of Hesse became the first state to declare compliant use to be possible (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 2025). Almost three years separate the result from the first sign of resolution.

In both cases an EU law identified the problem correctly. The solution came only after a member state put pressure for years and the firm changed its architecture and standards of regulation. Regulation made the exposure undeniable but did not produce the fix.

"Rules exclude firms from a tier but do not create firms to fill the tier."

Regulation Without Capacity

Brussels responds with more regulatory legislation. The GDPR, the NIS2 Directive, the Cybersecurity Act and the 2026 Tech Sovereignty Package form one sequence. The central piece of that is CADA, which separates cloud and AI services into four sovereignty levels. The first tier allows US hyperscalers to operate freely. The top-tier covers about 1% of public sector data and bars providers unless the Commission grants an exception (EUR-Lex, 2026). The Executive Vice-President Henna Virkkunen claims that the European Union wants to ensure that "nobody has a kill switch" over Europe's critical systems (Nicol-Schwarz, 2026).

Farrand and Carrapico (2022) call this regulatory mercantilism. CADA fits that definition. American law requires public buyers to favour domestic

suppliers, but CADA has no buy-European mandate, because the Commission was trying to dissuade US retaliation. They create no supplier to deliver to that tier.

Two design choices deepen the gap. Member states administer enforcement so a reasonable national reading allows the hyperscaler to win a sensitive contract. The control test also weighs nominal ownership, that is, who controls the shares, against effective control, or who controls how the system is running. Twenty-four European cloud CEOs under CISPE called this weakness 'sovereignty washing' (Hale, 2026).

The trend of "sovereignty washing" continued in April 2026. The Commission awarded its first sovereignty-scored cloud contract to four European companies under an eight-point Cloud Sovereignty Framework. Three winners are fully EU-owned. Proximus was the fourth, and it included S3NS, a joint venture between Thales and Google Cloud (European Commission, 2026). Legal exposure improved on paper. Supply continuity and time to remedy remained. A rule does not allow a firm to be part of a tier. A rule does not build a firm to fill the tier.

Regulatory Sovereignty and Operational Autonomy: One Framework, Two Layers

Edler et al. (2023) define technology sovereignty as the capacity to act, and this article adopts the definition as its single test.

Three measures worked in this case. Legal exposure to foreign compulsion is mostly in the authority layer. Supply continuity and time to remedy are in the capacity layer. Every case does not pass the test on at least one of these three measures. The Microsoft testimony cannot be viewed as legal exposure, as the contract and contract-bound data boundaries of the CLOUD Act still cover the law and are not in the reach of the CLOUD Act. The Health Data Hub fails on the other two: six years between the 2020 finding and the migration to Scaleway. Microsoft 365 fails to fix it in time: three and a half years between the German finding and the first sign of resolution. Legal exposure and supply continuity in the S3NS bid remain open.

Two layers follow. The authority layer is rule-setting within a jurisdiction, regulatory sovereignty. The capacity layer includes a buyer's freedom to refuse a supplier and keep functioning, which is operational autonomy. Pohle and Thiel (2020) draw a parallel line between control and capacity. Edler et al. warn of near autarky, so autonomy here means managed interdependence. Sensitive workloads need an exit option. General workloads do not.

Farrand and Carrapico (2022) explain why the authority layer is chosen. Rules provide for market position at low fiscal cost. In addition, Bradford (2019) predicts EU rules will change firm behaviour even more globally, and Microsoft's EU Data Boundary and Data Protection Addendum are in line with the prediction. Both changes reduced exposure to GDPR. CLOUD Act exposure, ownership and exit options stayed as before. The EU had an influence over the vendor and still relies on the vendor. The EU cloud share fell from 29 per cent in 2017 to 15 per cent in 2022 (Gundermann, 2026), and the GDPR and the Cybersecurity Act are in place. Scale, price and incumbent-default procurement led to the loss, and regulation did

not reverse the trend. The layers move independently, and there is no causal connection in either direction. Regulatory sovereignty has not led to operational autonomy.

What Closing The Gap Would Require

Closing the gap requires building all three measures together. Control rules deal with legal exposure, supply issues about continuity and buyer capacity is related to time to remedy. No measure comes first because each is fed back to the others. The Health Data Hub shows the loop. A number of officials felt there was no European provider of the scale of Azure, so the contract went to the incumbent. European providers remained small without major buyers. Six years passed before the data shifted (Marchandon, 2026). Ownership decides legal exposure. General workloads accept foreign-owned capacity, but those with sensitive tiers require EU oversight. That only works if we have control and EU enforcement in place. CADA has neither. Sovereign-by-construction platforms are somewhere in the middle between the tiers. Each has a domestic operator over foreign technology. France's Bleu, a subsidiary of Orange and Capgemini, will run Microsoft Azure and Microsoft 365 under French ownership (Bleu, 2026). Germany's Delos Cloud, an SAP subsidiary based on Azure, operates under BSI oversight (Bertelsmann, 2024). Nobody has tested whether this structure is effective in removing CLOUD Act exposure when an American firm licenses the technology in question. Neither of the platforms offers supply continuity, so they are transitional. The Dutch government has blocked Kyndryl from buying Solvinity, which hosts DigiD infrastructure. The block protects the legal exposure and does not add any capacity (Haeck, 2026).

Supply is the tightest constraint. Martens (2026) puts EU AI compute at about two gigawatts, or about 5 per cent of the global total, and expects planned projects to move the share little. Speed and grid access have to prohibit supply more than ownership. The Dutch sovereign cloud design shows managed interdependence in practice. The design aims for full software control and gives up hardware dependence (Loohuis, 2026); no European manufacturer ever makes CPUs, GPUs or ASICs.

Demand builds supply over time. In order to do so, procurement increases supplier capacity when buyers work together. Stojčić et al. (2020) find a large impact of procurement on innovation and output of 41,623 firms in 8 Central and Eastern European countries. Some EU member states are starting to take action on these findings. France will replace Microsoft Teams and Zoom with Visio by 2027 across state offices (Davies, 2026). Schleswig-Holstein moved nearly 80 per cent of state workplaces to LibreOffice by the end of 2025 (Krempl, 2025). Where policy has been certified or fined in the past, governments acquire and operate capacity, and other public bodies will reuse the result.

Organisations limit how far this goes. Uyarra et al. (2020) point to a lack of uptake of innovation procurement as being due to poor buyer capability, poor coordination and low incentives. The Dutch municipal platform Signalen has roughly 15 contributing municipalities, versus 30 to 40 needed for long-term sustainability (Linåker et al., 2026). A public sector with no technical staff cannot consider an exit option, let alone take one.

The improvements are partial. About 20 per cent of workplaces in Schleswig-Holstein still rely on Microsoft because specialised applications are built into Office (Krempl, 2025). Visio restricted meetings to 150 people in April 2026, and Teams to 10,000 people (GARO, 2026). France, Germany and the Netherlands also create separate platforms and work in parallel. This duplication doesn't violate Edler et al.'s warning. (2023) against autarky, as each state still relies on foreign hardware. Duplication does fragment the pooled demand, which raises scale. Managed interdependence points to shared builds at the EU level.

Policy Recommendations

Two follow from the framework. The first is the capacity layer. The second is connecting the authority layer to this capability.

The EU should co-finance shared, permanent public sector capacity instead of national builds of projects in parallel (European Commission, 2021). The capacity of Europe to support open source institutions is far too small compared to the value open source gives. Co-financing based on cross-border reuse of platforms such as openDesk fills this gap and eliminates the redundancy Edler et al. (2023) find in the three platforms in the French, German, and Dutch. Pooled builds are of a scale that no single state can sustain, ensuring the continuity of the supply chain. A common codebase removes the need to go through a new development cycle for each buyer, which can take much longer to fix. Signalen shows the mechanism. Municipalities contribute a third of development costs and Amsterdam sponsors the rest. The platform has only 15 contributors compared to the 30 to 40 we estimate long-term sustainability needs (Linåker et al., 2026). EU co-financing would close this gap.

Second, member states should tie procurement to the sovereignty tiers and write exit terms into every sensitive contract. Specific workloads accept foreign-owned capacity. Sensitive tiers need EU control, but it is by effective control and not nominal ownership which is relevant for legal exposure. There are sovereign-by-construction platforms like Bleu, Delos, and S3NS to take over in the transition period, and the foreign technology under them does not provide any supply continuity. Exit terms set the duration to be fixed in advance if needed. The large contracts are split into lots for smaller European companies and parallel running is provided for in the transition. The Data Act's prohibition on switching charges from 12 January 2027 is the foundation (European Commission, n.d.). Transition comes at a cost. The Dutch Cloud Community, a trade association of domestic providers, estimates three to five years of parallel operation and faults the STACKIT agreement for giving domestic providers no chance to compete (Loohuis, 2026).

Neither recommendation works alone. Tiers without domestic supply reproduce the S3NS result, and a sensitive contract still runs on a US platform. Shared capacity without binding tiers allows buyers to default to the incumbent, as the Health Data Hub did. ECIPE puts the EU-US ICT and cloud investment gap at around $1.36 trillion and calls the sovereigntist framing misguided. For this reason, domestic champions would bring in capital and talent from other industries to fill a gap of this size, and open, free, and non-discriminatory access to global cloud capacity is cheaper (Bauer et al., 2024).

The critique leaves the original exposure untouched. Cost doesn't change what the CLOUD Act requires an American firm to reveal, nor does it change what a foreign government will do to cut off. In doing so, researchers have not decided whether stronger contractual safeguards within an open architecture will reduce the exposure at lower cost. The tier-based design limits the question to sensitive workloads.

Conclusion

Setting the terms differs from controlling the infrastructure. A health database ran on Azure for six years after regulators found the arrangement unlawful. German public bodies kept using software their own regulators questioned, because no domestic alternative stood ready. Over the same period, the EU-based cloud share fell from roughly 29 to 15 per cent while the rulebook grew. Vendors changed their conduct under regulatory pressure, as the Brussels Effect predicts, yet buyers gained no option to leave.

The framework explains the pattern. Regulatory sovereignty sits in the authority layer and has advanced. Operational autonomy sits in the capacity layer and has stalled. Measured by legal exposure, supply continuity, and time to remedy, the main cases fail on at least one count.

Where the gap narrowed, member states did the work. France, the Netherlands, and Schleswig-Holstein acquired and operated capacity instead of certifying or fining. The EU role is narrower and still decisive: fund shared builds, set the control rule by tier, and force deadlines after findings.

The Tech Sovereignty Package is the most serious EU-scale response so far. Its flagship procurement nonetheless produced a winning bid running partly on Google Cloud. Rules exclude firms from a tier but do not create firms to fill the tier. Closing the gap demands supply, demand, and institutional capacity together, and member states have led that work with partial results. The next procurement round will test whether the EU builds capacity or writes more rules.

References

Bauer, M., Erixon, F., & Pandya, D. (2024, May 28). The EU's trillion dollar gap in ICT and cloud computing capacities: The case for a new approach to cloud policy. European Centre for International Political Economy. https://ecipe.org/publications/eu-gap-ict-and-cloud-computing/

Bertelsmann. (2024). First sovereign cloud platform for the German administration on the home straight. https://ber-cws-prod-web-release.azurewebsites.net/en/media/news/first-sovereign-cloud-platform-for-the-german-administration-on-the-home-straight.html

Bleu. (2026, May 15). Collaborer et innover en confiance. https://www.bleucloud.fr/

Bradford, A. (2019). The Brussels effect: How the European Union rules the world. Oxford University Press.

Congressional Research Service. (2025). Cross-border data sharing under the CLOUD Act (CRS Report No. R45173). https://www.congress.gov/crs-product/R45173

Davies, P. (2026, January 27). France to ditch US platforms Microsoft Teams, Zoom for 'sovereign platform' citing security concerns. Euronews. https://www.euronews.com/2026/01/27/france-to-ditch-us-platforms-microsoft-teams-zoom-for-sovereign-platform-amid-security-con

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. (2025, November 14). HBDI: Microsoft 365 kann datenschutzkonform genutzt werden. https://datenschutz.hessen.de/presse/hbdi-microsoft-365-kann-datenschutzkonform-genutzt-werden

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. Research Policy, 52(6), Article 104765. https://doi.org/10.1016/j.respol.2023.104765

European Commission. (n.d.). Data Act explained. Shaping Europe's Digital Future. Retrieved October 4, 2026, from https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

European Commission. (2021, September 21). Study about the impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and

European Commission. (2026a, April 17). European Commission awards €180 million tender for sovereign cloud to four European providers [Press release]. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_833/IP_26_833_EN.pdf

European Commission. (2026b). Proposal for a regulation on cloud and AI development (COM(2026) 502 final). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0502

European Data Protection Supervisor. (2024). European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies [Press release]. https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. European Security, 31(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Garo, A. (2026, April 13). La DINUM lâche Windows pour Linux et impose un plan de souveraineté à chaque ministère avant l'automne. IT Social. https://itsocial.fr/logiciel-agilite/logiciel-agilite-actualites/la-dinum-lache-windows-pour-linux-et-impose-un-plan-de-souverainete-numerique-a-chaque-ministere-avant-lautomne/

Gundermann, C. (2026, August 7). Brussels vs. Brussels: The EU's Data Act and the DMA's clash over cloud. Center for Strategic and International Studies. https://www.csis.org/analysis/brussels-vs-brussels-eus-data-act-and-dmas-clash-over-cloud

Haeck, P. (2026, May 26). Netherlands blocks US takeover of vital digital supplier. Politico. https://www.politico.eu/article/netherlands-blocks-us-takeover-vital-digital-supplier/

Hale, C. (2026, March 19). Dozens of European cloud CEOs call for real tech sovereignty ahead of Cloud and AI Development Act. TechRadar. https://www.techradar.com/pro/dozens-of-european-cloud-ceos-call-for-real-tech-sovereignty-ahead-of-cloud-and-ai-development-act

Interoperable Europe Portal. (2025). Open source for municipal services: Case study on Signalen. https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/open-source-municipal-services-case-study-signalen

Khafo, S. (2025). Procedure file 2025/2007(INI). Legislative Observatory, European Parliament. https://oeil.europarl.europa.eu/oeil/en/procedure-file?reference=2025/2007(INI)

Krempl, S. (2025, December 7). Goodbye, Microsoft: Schleswig-Holstein relies on open source and saves millions. Heise Online. https://www.heise.de/en/news/Goodbye-Microsoft-Schleswig-Holstein-relies-on-Open-Source-and-saves-millions-11105459.html

Linåker, J., Nummelin-Carlberg, A., & O'Riordan, C. (2026). Public sector open source program offices — Archetypes for how to grow (common) institutional capabilities. Journal of Systems and Software, 241, Article 112998. https://doi.org/10.1016/j.jss.2026.112998

Lomas, N. (2022, November 28). Microsoft 365 faces darkening GDPR compliance clouds after German report. TechCrunch. https://techcrunch.com/2022/11/28/microsoft-365-faces-darkening-gdpr-compliance-clouds-after-german-report/

Loohuis, K. (2026, September 24). Netherlands designs sovereign cloud but concedes hardware dependency. Computer Weekly. https://www.computerweekly.com/news/366651113/Netherlands-designs-sovereign-cloud-but-concedes-hardware-dependency

Marchandon, L. (2026, April 23). France swaps Microsoft for Iliad's Scaleway to repatriate health data hub. Reuters. https://www.reuters.com/world/europe/france-swaps-microsoft-iliads-scaleway-repatriate-health-data-hub-2026-04-23/

Martens, B. (2026, July 8). How can Europe address its pressing AI compute infrastructure shortfall? Bruegel. https://www.bruegel.org/policy-brief/how-can-europe-address-its-pressing-ai-compute-infrastructure-shortfall

McDermott Will & Emery. (2020, October 15). Transfers of health data from France to the United States not prohibited… but must be protected by strong safeguards. https://www.mcdermottlaw.com/insights/transfers-of-health-data-from-france-to-the-us-are-not-prohibited-by-the-french-data-protection-authority-or-french-courts/

Nicol-Schwarz, K. (2026, June 3). Europe unveils tech sovereignty package amid growing concerns over reliance on U.S. tech: "We want to be sure nobody has a kill switch." CNBC. https://www.cnbc.com/2026/06/03/europe-tech-sovereignty-us-tech-reliance.html

Pohle, J., & Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4). https://policyreview.info/concepts/digital-sovereignty

Sénat. (2025, June 9). CE commande publique : Compte rendu de la semaine du 9 juin 2025. https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html

Stojčić, N., Srhoj, S., & Coad, A. (2020). Innovation procurement as capability-building: Evaluating innovation policies in eight Central and Eastern European countries. European Economic Review, 121, Article 103330. https://doi.org/10.1016/j.euroecorev.2019.103330

Uyarra, E., Zabala-Iturriagagoitia, J. M., Flanagan, K., & Magro, E. (2020). Public procurement, innovation and industrial policy: Rationales, roles, capabilities and implementation. Research Policy, 49(1), Article 103844. https://doi.org/10.1016/j.respol.2019.103844

Foreign Affairs & Security Policy

Recent Publications



Our advisor Othmar Karas reflects on 25 years in EU governance, arguing that political will, not institutional flaws, holds the Union back from finishing the Single Market and building real sovereignty. His message to the next generation: "our future is in our hands."

Give it a read on our website!
>> Interview with Othmar Karas

This Month's EPIS Awards



Best Brief

Securing Europe's Supply of Raw Materials: Turning a European Dependency into A Strategic Asset
Eva Lan Montford & Tijn de Bruin

Best Blog

The Berlin Pride Attack and the Migration Myth How a German-born attacker's crime was used to blame migration - and what the evidence shows
Thomas Kurz

Best Report Article

UN Peacekeeping as a Site of Contestation: China and the Reshaping of the Global Order
Irene Olivo

Recent Accomplishments

As we strive to bring you additional value, we have lately started our Live Interview Series. Join us every week for talks with inspiring youth leaders, decisionmakers and experts, to gain new insights and learn more about their journey. Follow the announcements in the EPIS Network Chat!



Upcomming Publications

Next month, our FASP branch will release EPIS Reports on International Economic Relations and Eurasia. We will also bring you a the latest issue of the EPIS Magazine!

EPIS Thinktank
Report Groups

Join Us

Want to author the next EPIS Publication?

>> Apply for FASP Now!





Message Dmytro on WhatsApp. He will assist you :)

EPIS FASP Leader
fasp[at]epis-thinktank.com

Still got Questions ?

ARTIFICIAL INTELLIGENCE & CYBERSECURITY



AI Regulatory Divergence in Capitalist Regimes: A Comparative Analysis of the US, the EU and China.

Esperança Bennassar Rivero

About the Article

"The US shows a more flexible approach, the EU a more binding and rights-oriented framework, and China a stronger state-driven approach that does not overshadow its political principles."

About the Author

From a young age, Esperança has always had an enormous curiosity about the world beyond the borders of her home country. The multicultural environment in which she grew up fostered her passion for global politics, which led her to pursue a Bachelor's in International Studies. She is currently enrolled in an MSc in Politics and Technology, enhancing her technical skills in order to build a career in global public policy and governance.

Introduction

According to the Draghi Report (2024) on the future of European competitiveness, the European Union's underdevelopment in AI innovation is due to excessive regulation, mainly caused by the overlap of several European digital frameworks, such as the General Data Protection Regulation (GDPR), the Digital Services Act (DSA) and one of the most recent regulations, the EU AI Act, which entered into force in 2024 (Regulation (EU) 2024/1689). For this reason, the Digital Omnibus was proposed, with the aim of bringing relief to businesses through amendments to the current digital legislation (European Commission, 2025). However, the other two superpowers at the lead of the AI race —namely the United States and China—need not resort to such excessive regulatory measures.

These regulations are scarce in comparison to those of the EU: while there is no AI regulation at the federal level in the US and Artificial Intelligence Technologies (AIT) regulations remain strictly at the domestic level (White House, n.d.), the People's Republic of China (PRC) has only a few domestic initiatives that specifically target AI, such as the Interim Measures on Generative AI. However, albeit its voluntary core, it must be noted that the Chinese state promoted the Global AI Governance Initiative, encouraging countries to develop a people-centred approach to AI (Ministry of Foreign Affairs of the People's Republic of China, 2023). By contrast, the EU AI Act attempts to exercise binding force at an international level, showing a much stronger international stance.

Overall, the big picture suggests that the current AI regulatory frameworks are fragmented, with the US preserving regulation at a rather domestic level compared to the rest. The paper at hand will delve deeper into the regulatory differences among the three frameworks (the EU, China and the US) and will provide an explanation for such divergence based on the capitalist regime of each of the countries, drawing on the theory presented by Hall & Soskice (2001) and Nölke (2018).

Varieties of Capitalism is a theory arguing that economies differ systematically in how firms coordinate with other actors, therefore shaping institutions and policies.

The state of the debate

Paul (2022) has identified three main streams of literature regarding AIT's regulations: applied ethics and its main implications, the use of risk-analytical models to intervene in businesses and lastly, the politics behind AI regulation, with an emphasis on the role of capture by big tech businesses. However, the inclusion of capitalism into the frame expands the scope. In this way, four different streams of literature have been identified, relative to AIT regulation and its interplay with capitalist regimes.

Firstly, existing studies explore how actors at the lead of the AI race—primarily the EU, the US and China—regulate these technologies. Authors like Hilliard et al. (2026) focus on the complete landscape of AI policy initiatives worldwide, and highlight the similarities and differences between regulations. They find that horizontal laws converge on a risk-based

approach, but countries disagree on which systems are classified as "high-risk".

On the one hand, the EU AI regulatory framework is characterised as horizontal, risk-based and binding, which was unprecedented until recently. Ebers (2025) emphasises the importance and appropriateness of the risk-based component of the EU AI Act, along with the limitations of such an approach. More precisely, he mentions the complexity of reaching a consensus on the prioritisation of each risk, especially among different actors with diverse interests. On the other hand, the US relies on fragmented federal and state initiatives and sector-specific rules, with a lack of binding effect (White House, n.d.). Additionally, Sloane & Wüllhorst (2025) compare both frameworks against Canada's AI regulations, finding that transparency acts as the main mechanism for the effective mitigation of AI harms.

There is a third part of this specific stream of literature focused on the Chinese initiatives to regulate AI technologies, exemplified by authors such as Sheehan (2023) or Roberts et al. (2021). The former's investigation indicates that China's rules on algorithms are mainly shaped by the concern of the Chinese Communist Party (CCP) with controlling online content, even though it may also be influenced by scholars and international debates. Overall, the Chinese regulatory approach to AI is carried out by the state, oriented towards industrial promotion and politically driven. Simultaneously, the government may hold back from regulating these technologies in order to foster innovation (Zhang, 2024).

Secondly, the literature focuses on the ethical implications of AI and whether they are correctly addressed and covered by current AI regulatory frameworks. Principles such as transparency, accountability and privacy are the core of this stream. Corrêa et al. (2023) claim that the weight distributed to each principle diverges not only across countries, but also across the public sphere, the private sphere and NGOs within states. Furthermore, they provide a detailed explanation of the regulatory focus of each of the cases: the EU AI regulation is risk-based, the US AI regulation is based on the protection of individuals' rights alongside a preservation of national integrity, and China's AI regulation is extraterritorial and focuses on content moderation. Thus, this literature identifies some convergence in the ethical narrative surrounding AI, but this does not necessarily imply the existence of institutions with the same ability to enforce these principles.

Next, a third stream presents AI governance as a field where geopolitics and regulatory competition play a big role. Smuha (2019) claims that said "race to AI" also involves a "race to AI regulation". Additionally, Bradford (2020) coined the concept of "the Brussels Effect", which suggests that access to the EU market can encourage multinational companies to adopt European standards beyond EU territory.

Finally, a fourth stream investigates whether there is existing literature connecting capitalist regimes with AI regulation. To do so, topics from political economy and innovation were linked to AIT regulation. Mittelman (2022) examines the term "algorithmic capitalism" and how AI expands corporate and platform power. Similarly, Tallberg et al. (2024) focus on non-state actor

preferences on AI regulation in the EU. Next, Kulothungan et al. (2025) investigate whether AI regulation enhances or inhibits growth in capitalist economies. Closer to this study, we find Hayakawa (2026), who argues that contemporary capitalism is shaped by AI-driven governance. Then, Witt and Jackson (2016) examine the correlation between Varieties of Capitalism (VoC) theory and innovation. However, while these studies link capitalism to AI, none of them explains how different economic models shape the way countries regulate AI.

Capitalism as the missing variable

The previous literature review suggests that studies to date focus on explaining the content and diffusion of AI regulation, whereas less attention is given to whether economic institutions influence regulatory preferences. The purpose of this research is to extend VoC theory to AI regulation. The mechanism behind this is that capitalist institutions shape firm coordination and state-business relations, which in turn affect AI regulatory architecture.

The Varieties of Capitalism (VoC) approach, developed by Hall and Soskice (2001), posits that capitalist economies differ in their institutional arrangements, and that these differences give each economy divergent comparative advantages rather than converging on a single model. The authors define firms as central actors that have intrinsic coordination problems, which they identify in several dimensions, including corporate finance, relations between firms and employees and education and vocational training. Coordination refers in this instance to the way in which firms obtain capital, labour or technology from other actors. The authors distinguish two models of economies based on this coordination: Liberal Market Economies (LMEs)—such as the US, the UK or Canada—, where firms coordinate mainly through competitive market arrangements and hierarchies, and Coordinated Market Economies (CMEs)—such as Germany, Japan or Sweden—, where firms coordinate through non-market relationships, such as networks or business associations. Even though Hall and Soskice associate LMEs with radical innovation and CMEs with incremental innovation, Witt and Jackson (2016) find that radical innovation may emerge from hybrid institutions. Nevertheless, not all economies can conform to these two systems.

"While each case broadly aligns with its predicted model, strategic influences can divert regulatory actions from the predictions of each model."

Nölke (2018) extends Hall & Soskice's (2001) theory by adding another category to the scheme: State-Permeated Economies (SMEs). Firms' coordination in these economies depends more directly on relationships with public authorities, without the requirement of it being a centrally planned economy. In these economies, the state supports particular firms according to strategic priorities, while at the same time it keeps domestic firms competitive. Examples include most of the members of the BRICS, such as China and India.

All in all, the question of how these economic models regulate AI arises. They may influence how governments interact with companies, which is key to understanding more permissive

or more limited regulations. Additionally, the literature portrays the US as an LME, while China is classified as an SME. Although the European Union contains both CMEs and LMEs, it will be treated as a CME in this study for simplification, as it is mainly led by this group (Khan et al., 2026). Its largest economy, Germany, is the classic example of a CME, and EU policymaking itself is built on coordination similar to that of CMEs (Consolidated Version of the Treaty on the Functioning of the European Union [TFEU], 2016, Art. 154-155). However, one must not assume that the whole EU works strictly as a CME, as countries like Ireland are still classified as LMEs.

The three AI superpowers

This research attempts to evaluate whether current AI regulations in each of the case studies logically match hypotheses as to how each economic model behaves with regard to regulation. To do so, regulatory assumptions have been extracted for three common dimensions for each of the models – and the respective case studies associated with them – based on the theory that has been outlined above. The comparison focuses on the following dimensions: the form of regulation, the relationship between governments and companies and the balance between innovation and risk.

For LMEs, flexible labour markets and the importance of capital markets suggest a more adaptable regulatory environment. Regulation is expected to be less strict and more responsive to market interests, with companies maintaining a relatively independent relationship with governments. Given the focus on competition and disruptive innovation, I also expect more willingness to accept risks when they encourage technological development, potentially placing less emphasis on individual privacy rights.

For CMEs, stronger coordination and long-term relationships suggest a more stable and structured regulatory environment. Stricter and more homogeneous frameworks are expected, with a more interdependent relationship between governments and companies. The stronger emphasis on worker protection and bargaining also suggests greater attention to human rights and individual protections, with lower tolerance for risks that could undermine them.

For SMEs, the close relationship between public authorities and domestic corporations suggests a more state-driven regulatory environment. Therefore, regulation is expected to have a stronger political dimension and to adapt to state priorities and specific contexts. Finally, as the state can actively promote strategic sectors and technologies, I expect innovation to be more strongly guided by government priorities, with greater willingness to accept risks when they support strategic objectives.

Dimension	LME	CME	SME
Form of regulation	Flexible	Binding, coordinated	State-driven, context-specific
Government-company relationship	Relatively independent	Interdependent	Strong state involvemeent
Innovation vs. risk	Innovation-oriented	Rights-oriented	State-directed innovation

Figure 1. Expected AI Governance Characteristics across VoCs. Own elaboration.

Moving on to the actual AI regulatory measures taken by each of the case studies, the EU framework mostly corresponds to the expectations derived from the CME model. The AI Act establishes a binding and relatively

homogeneous regulatory framework based on different levels of risk, with a strong focus on fundamental rights and safety, reflecting the expectation that stronger workers' protections lower the tolerance for regulatory risk-taking. Companies are subject to clear obligations and public authorities have an important role in supervision, suggesting a more coordinated relationship between governments and companies. At the same time, innovation is encouraged within defined limits, supporting the expectation of a more cautious and gradual approach to technological development.

Consistent with LME expectations, US AI governance is more fragmented and flexible, and relies on voluntary instruments (rather than binding rules) such as the NIST AI Risk Management Framework (NIST, 2021), leaving companies room for flexibility. This reflects a more independent relationship between governments and companies, while firms are allowed to respond more quickly to technological developments according to market pressures. This strategy also places emphasis on innovation and competition, suggesting a greater willingness to accept certain risks in exchange for technological development. In contrast, individual rights protections are addressed through specific sector regulations—such as data privacy laws at the state level, as there is also no comprehensive national regulation in the country (DLA Piper, 2026)—instead of a cohesive federal rights framework.

Likewise, the Chinese framework supports several of the expectations associated with the SME model. In terms of regulatory form, Chinese AI governance has developed a series of context-specific measures rather than a general regulation applicable within its borders (Ding, 2025). The state plays a central role in regulating AI and defining the conditions under which companies can develop and use these technologies. At the same time, regulation is combined with the promotion of AI innovation and strategic technological development. This suggests that the government does not simply seek to limit risk, but rather attempts to direct innovation towards state priorities, resulting in a more politically driven and context-specific regulatory approach.

To visually compare the case studies with the expectations stated in Figure 1, the following figure places each case on an ordinal scale composed of five points for each dimension. The purpose of this division is to reflect relative standing, rather than quantified differences. In this way, end points suggest that a case clearly follows one dominant logic, intermediate points suggest that one logic dominates while elements of the other logic still remain, and the middle point suggests that both logics weigh roughly equally for that factor.

Image to follow

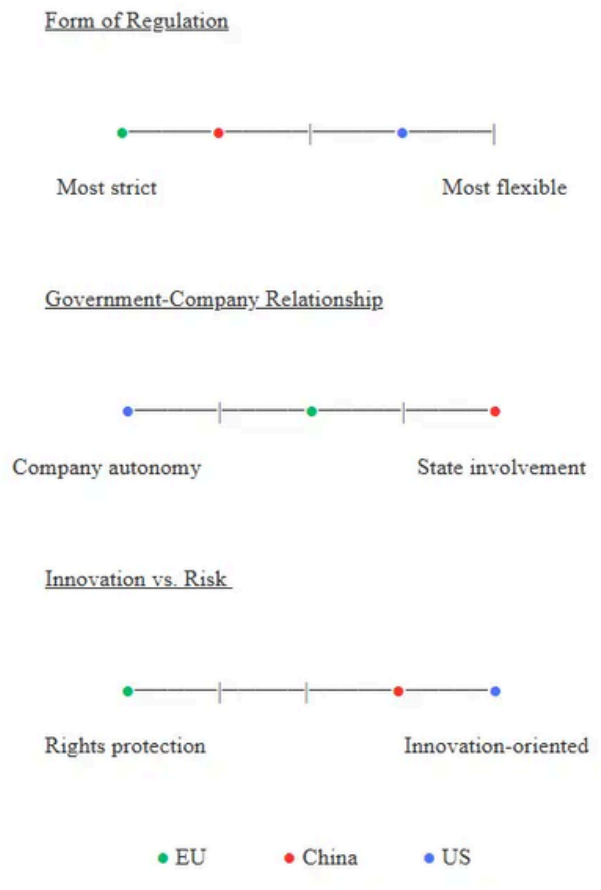


Figure 2. Positioning of the EU, China and the US across AI Governance Dimensions. Own elaboration. Positions are interpretive.

While each case broadly aligns with its predicted model, closer examination reveals points of friction. In the EU, the AI Act's risk-based approach leaves low-risk applications out of the frame for most obligations, introducing "free market" logic into a binding CME framework. In the US, reliance on voluntary frameworks does not necessarily translate into the absence of government involvement. For instance, Executive Order 14365 – which reinforces the purpose of establishing a unified national policy framework – signed under Trump's mandate states that the government can intervene in rolling out excessive laws that hinder innovation (White House, 2025). In China, the rules governing generative AI concerning content and ideology reveal political risk alongside the innovation-risk trade-off, highlighting a limitation of the study: political risk is a distinct regulatory factor that the innovation-risk aspect does not entirely cover. These tensions indicate that strategic influences can divert regulatory action from the predictions of each model when considered separately, despite the institutional logics remaining different.

Finally, the findings provide partial support for the expectations derived from the three models. The US shows a more flexible approach, the EU a more binding and rights-oriented framework, and China a stronger state-driven approach that does not overshadow its political principles. These differences broadly correspond to the expected forms of regulation and government–company relationships, but the frictions mentioned above also indicate that there are conflicting aspects within my hypotheses.

Does regulation follow capitalism?

Overall, the paper has examined whether the AI regulatory frameworks of each case study correspond to the expectations derived from their respective capitalist regimes. The findings suggest partial support for these theoretical expectations. The EU, as the exemplar CME, shows strong coordination in AI governance, with comprehensive regulations, coordination among different actors and a binding effect. The US, as the exemplar LME, presents a more fragmented approach, with no federal AI law and greater flexibility for companies to respond to different regulatory requirements across states. Finally, the PRC, as the exemplar SME, shows strong state involvement in AI regulation while simultaneously promoting innovation and

strategic technological development. Additionally, the US has demonstrated a rather domestic approach compared to the other two powers, which have shown greater interest in promoting their approaches to AI governance worldwide. Nevertheless, it must be noted that capitalist regimes cannot fully explain all differences observed, and that only three dimensions within each regime were considered, which is an important limitation of this study. While the form of regulation and the relationship between governments and companies broadly correspond to the stated expectations, the balance between innovation and risk is less clear, as all three cases promote technological development while addressing its associated risks. Therefore, the VoC framework provides a useful approach for understanding differences in AI regulation, but should not be considered the only explanation of regulatory choices. Competitive and other economic factors may also influence the pace and manner in which governments shape their regulation.

References

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Consolidated version of the Treaty on the Functioning of the European Union. (2016). http://data.europa.eu/eli/treaty/tfeu_2016/oj

Corrêa, N. K., Galvão, C., Santos, J. W., Pino, C. D., Pinto, E. P., Barbosa, C., Massmann, D., Mambrini, R., Galvão, L., Terem, E., & Oliveira, N. de. (2023). Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. Patterns, 4(10), Article 100857. https://doi.org/10.1016/j.patter.2023.100857

Ding, L. (2025). China's regulation of artificial intelligence – progress and challenges. International Bar Association. https://www.ibanet.org/China-Regulation-of-Artificial-Intelligence-Progress-and-Challenges

DLA Piper. (2026). Data protection laws in the United States. https://www.dlapiperdataprotection.com/?t=law&c=US

Draghi, M. (2024). The Draghi report on EU competitiveness. European Commission. https://commission.europa.eu/topics/competitiveness/draghi-report_en

Ebers, M. (2025). Truly risk-based regulation of artificial intelligence: How to implement the EU's AI Act. European Journal of Risk Regulation, 16(2), 684–703. https://doi.org/10.1017/err.2024.78

European Commission. (2025). Digital omnibus regulation proposal. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

Hall, P. A., & Soskice, D. (Eds.). (2001). Varieties of capitalism: The institutional foundations of comparative advantage. Oxford University Press. https://academic.oup.com/book/301

Hayakawa, H. (2026). AI-driven capitalism and the transformation of democratic governance: Financialization, platform power, and blended sovereignty. SSRN. https://doi.org/10.2139/ssrn.6923278

Hilliard, A., Gulley, A., Kazim, E., & Koshiyama, A. S. (2026). Artificial intelligence policy worldwide: A comparative analysis. Royal Society Open Science, 13(2), Article 242234. https://doi.org/10.1098/rsos.242234

Khan, H., Stylianou, K., Khan, Z., & Wood, G. (2026). Strategic responses of platform multinational enterprises: Rethinking competition policy through a comparative institutional perspective. Long Range Planning, 59(3), Article 102636. https://doi.org/10.1016/j.lrp.2026.102636

Kulothungan, V., Mohan, P. R., & Gupta, D. (2025). AI regulation and capitalist growth: Balancing innovation, ethics, and global governance. In 2025 IEEE 11th Conference on Big Data Security on Cloud (BigDataSecurity) (pp. 39–45). IEEE. https://doi.org/10.1109/BigDataSecurity66063.2025.00020

Ministry of Foreign Affairs of the People's Republic of China. (2023). Global AI governance initiative. https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367503.html

Mittelman, J. H. (2022). The power of algorithmic capitalism. International Critical Thought, 12(3), 448–469. https://doi.org/10.1080/21598282.2022.2070858

NIST. (2021). AI RMF development. https://www.nist.gov/itl/ai-risk-management-framework/ai-rmf-development

Nölke, A. (2018). Dependent versus state-permeated capitalism: Two basic options for emerging markets. International Journal of Management and Economics, 54(4), 269–282. https://doi.org/10.2478/ijme-2018-0026

Paul, R. (2022). The politics of regulating artificial intelligence technologies: A competition state perspective. SSRN. https://doi.org/10.2139/ssrn.4272867

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (2024). http://data.europa.eu/eli/reg/2024/1689/oj

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation. In L. Floridi (Ed.), Ethics, governance, and policies in artificial intelligence (pp. 47–79). Springer. https://doi.org/10.1007/978-3-030-81907-1_5

Sheehan, M. (2023). China's AI regulations and how they get made. Horizons: Journal of International Relations and Sustainable Development, (24), 108–125.

Sloane, M., & Wüllhorst, E. (2025). A systematic review of regulatory strategies and transparency mandates in AI regulation in Europe, the United States, and Canada. Data & Policy, 7, Article e11. https://doi.org/10.1017/dap.2024.54

Smuha, N. A. (2019). From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. SSRN. https://doi.org/10.2139/ssrn.3501410

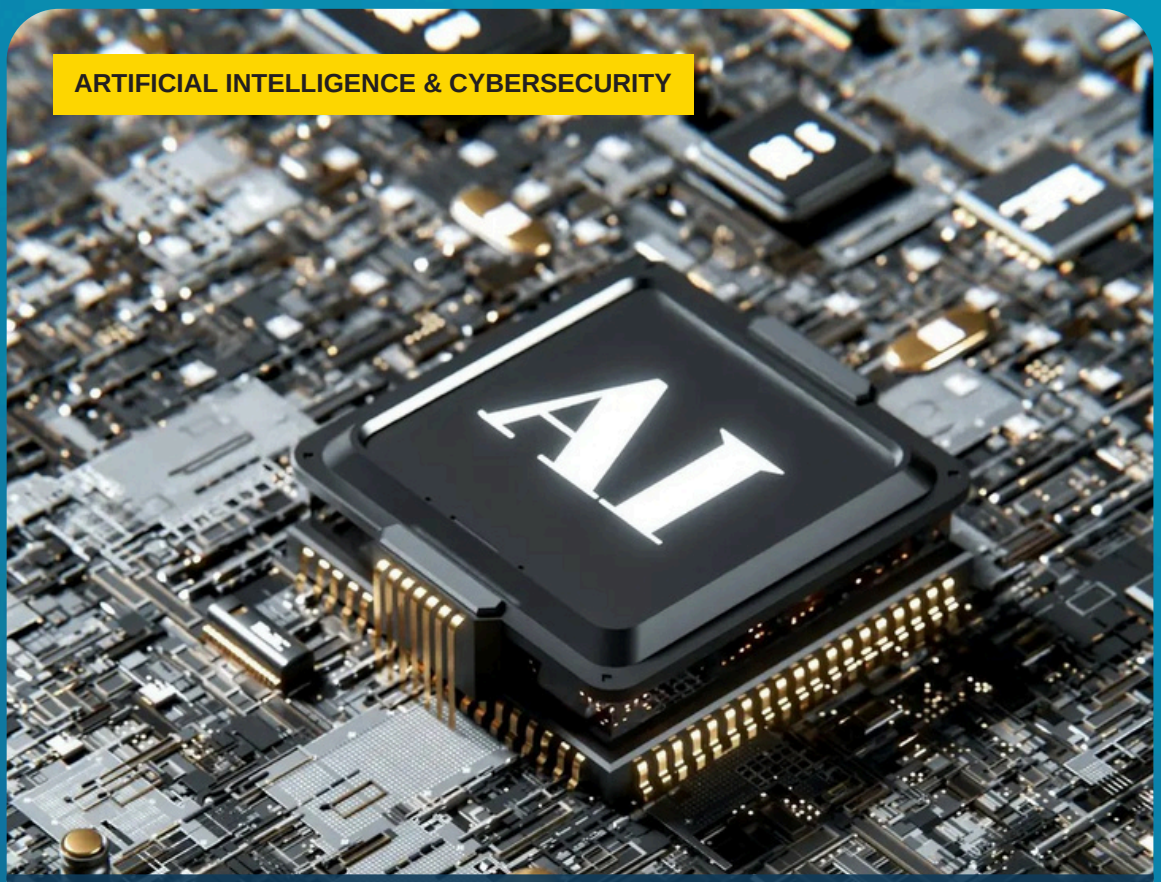
Tallberg, J., Lundgren, M., & Geith, J. (2024). AI regulation in the European Union: Examining non-state actor preferences. Business and Politics, 26(2), 218–239. https://doi.org/10.1017/bap.2023.36

White House. (n.d.). Artificial intelligence for the American people. https://trumpwhitehouse.archives.gov/ai/ai-american-worker/

White House. (2025, December 11). Ensuring a national policy framework for artificial intelligence. https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/

Witt, M. A., & Jackson, G. (2016). Varieties of capitalism and institutional comparative advantage: A test and reinterpretation. Journal of International Business Studies, 47(7), 778–806. https://doi.org/10.1057/s41267-016-0001-8

Zhang, A. H. (2024). The promise and perils of China's regulation of artificial intelligence. SSRN. https://doi.org/10.2139/ssrn.4708676



Economic Coordination and AI: Does AI Shift the Balance Between Markets and Planning?

Fabian Wylczoch

About the Article

"Nevertheless, the evidence considered here suggests that AI shifts the boundary between planning and markets rather than eliminating either."

About the Author

Fabian did his Bachelor's and Master's degree in industrial engineering at KIT in Karlsruhe. There, he focused on statistics, econometrics and macroeconomics. He has a profound interest in international relations and economics as well as in tech tech. He pursued an internship in a Tel Aviv tech startup where he was in contact with the DIW.

Introduction

Artificial intelligence has stirred up a longstanding debate over economic coordination. Market-driven systems mainly depend on decentralised choices, competition, and prices, whereas centrally planned systems use political objectives and administrative direction to guide production and investment. These are ideal types, not accurate representations of real economies. State and market each play a role in coordination. Market systems involve government intervention through infrastructure provision and regulation of strategically important sectors. At the same time, state-controlled economies also rely extensively on firms, markets, and prices. The main issue is whether AI leads to one pure type prevailing over the other or alters the relative advantages of centralised versus decentralised coordination.

The ability to collect and process data on a very large scale, which early planners could not even imagine, is one of AI's strongest capabilities. Besides gathering and processing information, AI excels at detecting patterns, predicting demand, optimising logistics, and supporting decisions. This seems to challenge the longstanding claim that economic knowledge is so widely dispersed that it precludes central control. On the other hand, AI can also empower decentralised decision-makers, enabling individuals and companies to analyse information affordably, obtain advice, and experiment with different approaches. This literature-based article addresses two questions: first, whether AI provides a greater net benefit to centrally planned or market systems; and second, whether it poses a risk to the future of market-driven societies. It argues that AI enables central coordination of a larger number of activities, especially when objectives are clearly measurable and operating conditions relatively stable.

However, market systems are not free from AI's influence. Economies of scale in computing infrastructure, data, and technical capabilities can favour larger firms and contribute to market concentration (Brynjolfsson & Hitzig, 2025). Furthermore, if many decision-makers rely on similar models or information sources, their recommendations can become increasingly aligned, reducing diversity in decision-making (Burton et al., 2024). AI may also facilitate information manipulation. The likely outcome is not the disappearance of markets but the emergence of hybrid systems combining AI-supported planning and decentralised experimentation.

Knowledge Problem: the difficulty of central authorities accessing and using dispersed, local, and tacit information held by individuals across an economy.

Foundations of Economic Coordination

The classical debate concerns more than a government's ability to process information. Mises argued that comprehensive socialist planning creates an economic calculation problem. If capital goods are not traded on markets, their prices cannot be established through exchange, leaving planners without a way to compare alternative uses of scarce resources. Greater computational power can

improve arithmetic but cannot itself produce the value judgements that emerge through market exchange (Mises, 1920). Lange argued that a socialist economy could retain consumer demand and use administrative prices. By raising prices when supply falls short and lowering them when supply exceeds demand, a central planning authority could approach market equilibrium through trial and error (Lange, 1938). Lange's model is particularly relevant to AI because machine learning could speed up feedback and allow adjustments across more variables than human administrators could handle.

Hayek's position was broader than Mises' or Lange's arguments. Economically significant information, such as local changes in demand, available inventories, specific production capacities, temporary shortages, or local consumer preferences, is scattered among many people and often relates to a particular time or place. Market prices reflect the scarcity of resources, enabling people to make production decisions without knowing the entire economy or understanding every shortage or surplus. As such, competition is not only a means of finding solutions but also a process of discovery through which knowledge, preferences, and opportunities are revealed (Hayek, 1945).

Even a very powerful computer, such as an AI system with access to vast amounts of recorded history, cannot be assumed to discover everything that decentralised actors might uncover. An AI system may identify previously unknown patterns or relationships within existing data, but this is different from generating new economic knowledge through experimentation and interaction. When comparing planning systems, four dimensions need to be distinguished: (1) the extent to which they can be supplied with and process information; (2) the incentives to disclose information honestly and act efficiently; (3) the degree to which they can adapt to changing circumstances and discover new possibilities; and (4) the way political and economic power is distributed.

Artificial intelligence is most directly likely to increase the effectiveness of the first dimension because gathering data, identifying patterns, and processing large quantities of information are among its core technical capabilities. The remaining three dimensions depend not only on computational capacity, but also on incentives, experimentation, institutional feedback, and the distribution of authority. AI can influence these factors, but it does not automatically improve them (Hayek, 1945; Zou, 2025).

Artificial Intelligence as a Tool of Economic Coordination

Generative AI drastically reduces the cost of turning large volumes of data into forecasts, classifications, recommendations, and content. It can also centralise organisational decision-making by enabling a smaller number of managers to analyse information and make decisions across a wider span of a business. AI-generated insights have become more affordable as advanced analytical capabilities are made available to more people. Sourav et al. (2025) identify data inequality, employment losses, and weak regulation as potential obstacles to inclusive growth. They also report cross-country links between AI and growth, but these links do not prove that AI alone causes economic growth (Sourav et al., 2025). Brynjolfsson and Hitzig (2025) suggest that AI

can help knowledge to be shared across organisations, enabling central management to make efficient decisions even when dealing with very large teams. The result could favour larger companies, increase industry concentration, and reduce the authority of line managers.

Similarly, AI might improve collective intelligence by giving individuals better access to information and analytical support (Burton et al., 2024). Yet, if not managed carefully and equitably, it may threaten employment, while data inequality and weak governance remain obstacles to inclusive growth (Sourav et al., 2025).

"The key implication is that AI does not create a general advantage for one economic system: its effect depends on the characteristics of the economic problem being addressed."

AI should not be understood as a neutral economic tool. The quality and direction of AI-generated decisions are influenced by factors such as the dataset, measurement system, model design, objectives assigned to it, and the human choices behind these elements. Data reflect what was recorded previously and, as history shows, may be incomplete, biased, outdated, or deliberately manipulated to serve particular interests. As AI learns from past records to make predictions about the future, the use of historical data to predict outcomes is conceptually different from identifying genuinely new products, preferences, or production methods. Zou (2025) therefore distinguishes data from knowledge, prediction from discovery, and prices simulated by a model from real market prices.

AI's ability to produce very large volumes of output at the same time is a major advantage, but it is also a risk because errors and insights can both be amplified. When many decision-makers rely on a single model, their recommendations tend to become highly aligned, leading to a reduction in diversity of thought. Large language models (LLMs) could improve individuals' abilities, yet they might also increase uniformity in how people think, encourage reliance on automation, or lead people to agree before the underlying questions have been properly examined (Burton et al., 2024). In this way, AI redefines the capabilities of planning and markets. Economic outcomes depend particularly on three factors: who manages these systems, which goals they are designed to achieve, and whether their decisions can be reviewed and challenged.

Figure 1 summarises the different information-processing logic underlying market coordination and AI-assisted planning. In markets, local knowledge enters the coordination process through individual decisions, exchange, prices, and profit-and-loss feedback, allowing dispersed actors to adjust independently. AI-assisted planning instead channels economic data through centralised collection, model-based analysis, administrative decisions, and reported outcomes. The figure therefore illustrates the central argument of this paper: AI can substantially strengthen centralised information processing, but it does not remove the importance of how information is generated, communicated, and corrected within the underlying institutional system (Hayek, 1945; Brynjolfsson & Hitzig, 2025; Zou, 2025).

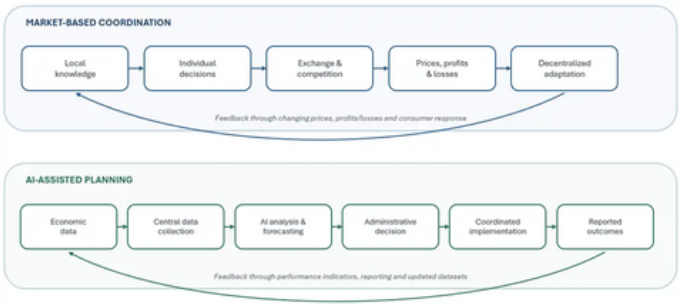


Figure 1. Information Processing in Market-Based and AI-Assisted Planning Systems. Based on Hayek (1945), Burton et al. (2024), Brynjolfsson & Hitzig (2025), and Zou (2025).

Opportunities and Risks for Centrally Planned Systems

AI can address one of central planning's greatest historical weaknesses: its limited capacity to gather, update, and interpret information. Governments can pool data on production, transport, energy, trade, and consumption, identify bottlenecks, and update policies more quickly. AI may be particularly useful where targets are clear, but interdependencies are high, such as electricity distribution networks, transport infrastructure, emergency logistics, or long-term industrial investment. By coordinating these projects across different sectors, governments can avoid duplication, ensure that resources are used efficiently, and help separate initiatives support each other.

China's 2017 New Generation Artificial Intelligence Development Plan illustrates how AI can form part of a national strategy. It identifies implications for economic competitiveness, national security, industrial development, and governance, and sets goals through 2030 (State Council of the PRC, 2017). AI could also make Lange-style adjustments faster and more responsive by detecting shortages in real time and updating administrative targets.

Non-democratic planning in the era of AI can have advantages, but this does not mean that it is necessarily justified or that it improves people's well-being. AI cannot determine whose interests to prioritise when defining social welfare or how growth should be balanced against equality, privacy, or environmental protection. These issues are questions of political choice, not ones that can be solved simply through technical optimisation. Furthermore, data supplied to central authorities can be manipulated if officials and organisations are rewarded by the government for meeting quotas. A model trained on faulty indicators could make such manipulation more systematic, while an error in a central model might end up affecting the whole economy (Zou, 2025).

Large concentrations of data, processing power, and surveillance capabilities can also result in greater state control. Chinese facial-recognition development not only serves government needs but also fuels private-sector innovation in advanced monitoring technology. This creates an "AI-tocracy" loop (Beraja et al., 2021). Planning does not logically require autocratic government. Nevertheless, centralised planning combined with AI-based surveillance can amplify the power of organisations that determine targets and evaluate compliance. AI might therefore help governments implement decisions efficiently without giving citizens more power to question them.

At the same time, we cannot ignore that the world economy is characterised by substantial interdependence. A country's ability to access

the latest chips, cloud computing infrastructure, data storage, and highly skilled workers is increasingly part of geopolitical competition. Consequently, even governments seeking greater planning capacity may remain dependent on a small number of private firms and foreign suppliers (Wasi et al., 2025). Moreover, cooperation between governments and large corporations can make lines of accountability less clear. When power and responsibility are distributed across public and private institutions, citizens may find it more difficult to determine which actor is responsible for particular decisions (Csernatoni et al., 2025).

Opportunities and Risks for Market-Based Systems

AI also supports the decentralised advantages of market economies. Individuals and firms can use it to explore markets, develop products, write code, conduct research, and experiment with ideas at lower cost. Rather than replacing local expertise, AI can assist the "person on the spot" by providing information and tools where decisions are made. Competition enables different actors to use models in their own ways, compare outcomes, and discard unprofitable approaches. Failures can remain local instead of affecting the entire system.

The impact on collective intelligence is likely to be beneficial when AI improves individual competence and groups maintain diverse information and alternatives (Burton et al., 2024). Under radical uncertainty, decentralised experimentation becomes especially valuable if relevant options and preferences are initially unknown. AI can reduce experimentation costs, but markets still provide feedback through voluntary exchange, allowing different interpretations to be tested. However, market economies cannot be equated with decentralised control. Frontier AI requires major investments in computing infrastructure, data, and technical skills.

These economies of scale and scope can lead to market dominance, centralised decision-making within firms, and less autonomy for employees and smaller competitors (Brynjolfsson & Hitzig, 2025). Technology firms are increasingly influential in critical infrastructure, communication channels, and platforms, prompting governments to pursue new forms of tech diplomacy (Cotroneo & Csernatoni, 2025). This may resemble market-based planning, with a few corporations rather than the state controlling key information and economic opportunities.

AI may also weaken the independence and diversity of individual decision-making when personalised recommendation systems and generated content systematically influence the information consumers encounter. The concern is not that decision quality can be reduced to a single measurable indicator, but that individuals may make choices within an increasingly curated and potentially manipulated information environment. Generative AI lowers the barrier to producing credible disinformation and may facilitate electoral interference, mass-persuasion campaigns, and digital authoritarianism. Meanwhile, the extraordinary market dominance of large platforms gives private firms considerable power over democratic deliberation (Csernatoni, 2024).

Consumer sovereignty within digital markets weakens when available choices and the

information surrounding them become opaque and curated by platforms. Lastly, uneven access to data and AI-enabled applications could widen differences in productivity and income, while automation could threaten specific types of employment (Sourav et al., 2025). Market mechanisms might enable entrepreneurial adoption of AI while making markets less competitive, less pluralistic, and less individualistic in practice.

Comparative Assessment

AI's relative advantage depends on the nature of the task to which it is applied. Central coordination will probably be most useful where outcomes can be measured, objectives are shared, the necessary data are available in one place, and activities need to be synchronised.

Figure 2 translates this distinction into a task-based framework. AI-assisted planning can offer relative advantages for activities with a high need for coordination but comparatively limited uncertainty, while decentralised market coordination retains advantages where uncertainty and the need for discovery are high. Where both coordination requirements and uncertainty are substantial, the figure points to a hybrid approach that combines public coordination with decentralised experimentation. The key implication is that AI does not create a general advantage for one economic system; its effect depends on the characteristics of the economic problem being addressed.

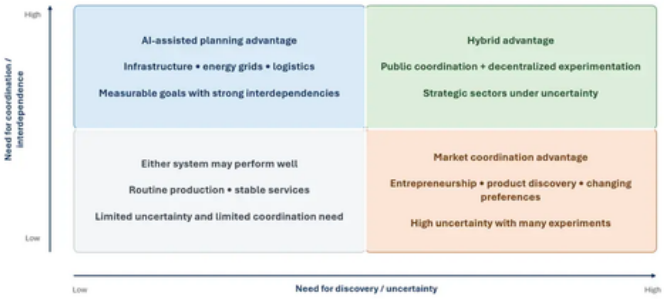


Figure 2. Relative Advantages of AI-Assisted Planning and Market Coordination by Task Characteristics. Based on Hayek (1945), Zou (2025), and Brynjolfsson & Hitzig (2025).

Infrastructure networks, inventories, logistics, and some aspects of industrial policy illustrate this logic. AI can increase the speed and scope of planning in these fields.

Decentralised coordination retains its relative strengths where demand, technology, or local conditions change rapidly; expertise is highly specialised and difficult to transfer; stakeholders have conflicting goals; and innovation results from many individual experiments. Markets do more than process a fixed set of information. Prices and competition also motivate people to reveal information, discover alternatives, take risks, and face the consequences of their decisions. AI may facilitate this process but cannot eliminate the need for institutional feedback, incentives, and contestability (Hayek, 1945; Zou, 2025).

The marginal benefit of AI may be especially visible in planned systems because it alleviates a longstanding technical constraint: the limited ability of a central authority to gather, update, and process large volumes of dispersed economic information. This does not mean that their overall performance will exceed that of market economies. Market actors also adopt AI, often rapidly, and can combine it with

decentralised experimentation. Market concentration may allow a few corporations to capture much of the benefit, while a central state may coordinate strategically but suppress inconvenient information.

The greatest net advantage is therefore likely to accrue neither to a purely planned economy nor to an unregulated market. It is more likely to arise in systems that combine capable public coordination with competitive discovery: governments can establish infrastructure, rules, and long-term objectives, while independent firms and individuals retain the freedom to experiment and challenge existing models. Importantly, public coordination and regulation do not necessarily eliminate experimentation; the relevant question is whether institutions leave independent actors sufficient room to test alternative approaches and challenge existing solutions. The decisive institutional properties are not simply "state" or "market", but diversity, accountability, adaptability, and the possibility of correcting errors.

Discussion

Artificial intelligence is unlikely to cause the collapse of market-driven, individualistic societies. Even so, it weakens the claim that large-scale coordination must necessarily be crude. AI enables governments and large corporations to monitor and manage more operations, at least in certain settings. Lange's (1938) iterative method is now more technically plausible because feedback can be processed continuously.

This development is not sufficient to dismiss or resolve all of Mises' or Hayek's objections. A computer's ability to reproduce capital prices meaningfully depends on authentic transactions actually taking place. Moreover, the knowledge behind a decision to buy or sell is not merely data that has been collected and stored; much of it is created through people's choices, negotiations, creativity, and reactions to results (Mises, 1920; Hayek, 1945). Besides, efficiency itself cannot be disentangled from the question of who actually controls the goals of an AI system and who has the right to challenge them.

Market societies should be concerned about what AI might bring. If data, computing, and information resources are controlled by a few actors, AI could reconcentrate economic authority even without formal state planning. This could undermine the independent judgement and diversity of views that both free markets and democracy rely on. The conflict today is not merely between an all-knowing state and a free individual; it is also about which systems of algorithmic coordination can be challenged and which cannot.

In the end, a combination of different systems is the most probable outcome: AI-supported public planning in areas or industries requiring large amounts of capital and infrastructure, potentially extensive planning within firms, and market-based experimentation especially where consumer preferences and technology remain uncertain because these conditions provide room for innovation and development. Whether freedom and prosperity can be ensured under such an arrangement will largely depend on competitiveness, public transparency, privacy protection, legal frameworks that keep different actors in check, and access to AI. Because much of the literature is recent and partly conceptual, any conclusion remains provisional.

Nevertheless, the evidence considered here suggests that AI shifts the boundary between planning and markets rather than eliminating either. Its greatest effect may be to increase the value—and the danger—of concentrated coordination while making the preservation of decentralised discovery and democratic accountability more important.

References

Beraja, M., Kao, A., Yang, D. Y., & Yuchtman, N. (2021). AI-tocracy (NBER Working Paper No. 29466). National Bureau of Economic Research. doi:10.3386/w29466

Brynjolfsson, E., & Hitzig, Z. (2025). AI's use of knowledge in society. In A. K. Agrawal, E. Brynjolfsson, & A. Korinek (Eds.), The economics of transformative AI (pp. 301–330). National Bureau of Economic Research.

Burton, J. W., Lopez-Lopez, E., Hechtlinger, S., Rahwan, Z., Aeschbach, S., Bakker, M. A., Becker, J. A., Berditchevskaia, A., Berger, J., Brinkmann, L., Flek, L., Herzog, S. M., Huang, S., Kapoor, S., Narayanan, A., Nussberger, A.-M., Yasseri, T., Nickl, P., Almaatouq, A., . . . Hertwig, R. (2024). How large language models can reshape collective intelligence. Nature Human Behaviour, 8(9), 1643–1655. doi:10.1038/s41562-024-01959-9

Cotroneo, C., & Csernatoni, R. (2025). Tech diplomacy 2.0: Examining the intersections between industry and governments in international relations. International Journal of Cyber Diplomacy, 6, 3–18. doi:10.54852/ijcd.v6y202501

Csernatoni, R. (2024, December 18). Can democracy survive the disruptive power of AI? Carnegie Endowment for International Peace.

Csernatoni, R., Broeders, D., Andersen, L. H., Hoijtink, M., Bode, I., Lindsay, J. R., & Schwarz, E. (2025). Myth, power, and agency: Rethinking artificial intelligence, geopolitics and war. Minds and Machines, 35(3), Article 37. doi:10.1007/s11023-025-09741-0

Hayek, F. A. (1945). The use of knowledge in society. The American Economic Review, 35(4), 519–530.

Lange, O. (1938). On the economic theory of socialism. In B. E. Lippincott (Ed.), On the economic theory of socialism (pp. 55–143). University of Minnesota Press.

von Mises, L. (1920). Economic calculation in the socialist commonwealth. Ludwig von Mises Institute.

Sourav, M. S. A., Asha, N. B., & Reza, J. (2025). Generative AI in business analytics: Opportunities and risks for national economic growth. Journal of Computer Science and Technology Studies, 7(11), 224–247. doi:10.32996/jcsts.2025.7.11.22

State Council of the People's Republic of China. (2017). New generation artificial intelligence development plan (G. Webster, R. Creemers, E. Kania, & P. Triolo, Trans.). DigiChina.

Wasi, A. T., Eram, E. H., Mitu, S. A., & Ahsan, M. M. (2025). Generative AI as a geopolitical factor in Industry 5.0: Sovereignty, access, and control [Preprint]. arXiv.

Zou, H.-F. (2025). AI, central planning, and Hayek's knowledge problem: Why "The use of knowledge in society" survives the age of artificial intelligence (CEMA Working Paper No. 808). China Economics and Management Academy, Central University of Finance and Economics.

ARTIFICIAL INTELLIGENCE & CYBERSECURITY



Finland’s Comprehensive Security Concept and its Strategic Applications for Stronger AI Readiness

Sonja Liukkonen

About the Article

“Finland’s role in defending European and Alliance security is crucial because of its long eastern frontline.”

About the Author

Sonja Liukkonen is a multilingual master's student at Sciences Po Grenoble with an interdisciplinary background in international relations, geopolitics as well as languages including French and Chinese. She was educated at the University of Turku, Sciences Po Rennes, and Sciences Po Aix-en-Provence. Her master's thesis focuses on Europe–China relations and political discourse analysis. She has EU and diplomatic experience from the Embassy of Finland in Brussels and as a Blue Book trainee.

Due to Finland's challenging geographical landscape, often described as the land of thousands of lakes and forests, and its extensive land territory and small population, covering only 0.07% of the world's population, security and crisis preparedness questions have played a central role in Finnish society during the 20th century. This has led Finland to build its defence capabilities on mandatory military service for men, introduced in February 1919, and on its ability to rapidly transform its peacetime strength into wartime strength in just a few days (Army Command Finland, 2019).

Comprehensive security can be defined as cooperation among authorities, the business community, citizens, and organisations to share the responsibility for society's vital functions.

These questions matter more in modern Finnish society, as Finland has the longest eastern border among EU countries, accounting for 1,340 kilometres (Ministry of the Interior, 2026a). Since Finland joined NATO on 4 April 2023 (Ministry for Foreign Affairs of Finland, n.d.), this border has gained a new dimension. NATO's land border with Russia has roughly doubled in length. Finland's NATO membership, along with Sweden's, was a significant milestone in Northern Europe's politico-military geography as Euro-Atlantic deterrence's role grows in the region (Pesu, 2023). This shift has led Finland into a new phase of foreign policy, after decades of neutrality during the Cold War, followed later by military non-alignment (Kyllönen, 2025).

The new European security landscape, marked by hybrid threats, crises, and war, has drawn international attention to Finland, known for its crisis preparedness methods and comprehensive security concept. This shift in the security environment has led the Finnish government to introduce the renewed Security Strategy for Society in January 2025 to ensure society's security in all circumstances (Ministry of Defence, 2025).

Firstly, this article introduces Finland's changing security landscape since Russia's invasion of Ukraine on 24 February 2022, which marked a turning point towards Finland joining NATO. Secondly, this article explains Finland's unique comprehensive security concept and its applications. Thirdly, this article provides a brief overview of Finland's AI readiness and how Finland uses artificial intelligence to enhance social resilience. Overall, the article addresses the following research question: How do Finland's pre-existing higher levels of AI readiness reflect in higher societal resilience and defence sector innovation?

Finland's changing security landscape

The nature of warfare has changed in the early 21st century as it has gained a new dimension, notably hybrid warfare, whose importance is growing. The term refers to combinations of political, military, economic, and other non-physical actions used to achieve political objectives. Hybrid warfare can include cyberattacks, information operations, physical strikes aimed at creating uncertainty among citizens, and economic coercive measures. One key feature of hybrid warfare is its unpredictability. Normally, hybrid warfare is not

declared directly, which makes the line between peace and warfare uncertain (Salonius-Pasternak & Limnéll, 2015).

Finland's significant role in countering hybrid threats is reflected in the establishment of the Centre of Excellence for Countering Hybrid Threats in Helsinki in April 2017. This centre builds counter-hybrid capacity and trains participants from academia and the public, private, civil and military sectors (European Centre of Excellence for Countering Hybrid Threats, n.d.).

Events in Ukraine, beginning with Russia's annexation of Crimea in 2014, signalled to Finland the need to strengthen its societal preparedness, especially its comprehensive security concept, a core part of responding to hybrid warfare because it covers all forms of society. According to experts, Finland is well placed to respond to the threats posed by hybrid warfare, but it must strengthen its society's psychological and physical resilience, as well as its non-physical performance. These changes should be included in Finland's Security Strategy for Society in order that Finland can respond more effectively to power cuts, withstand the effects of cyberattacks, and better filter impactful information (Salonius-Pasternak & Limnéll, 2015). Since 2022, Finland has also increased its defence expenditure.

Image to follow

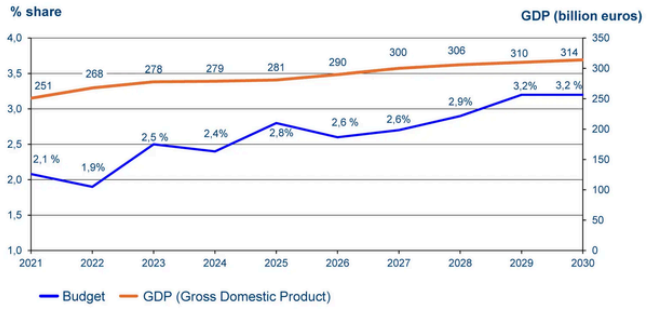


Figure 1. Defence expenditure as a percentage of GDP of Finland. Source: Ministry of Defence (n.d.).

Finland increased its defence sector expenditure to 2.5% from 2.1% (2021) right after expressing its interest in joining NATO on 17 May 2022 (Ministry for Foreign Affairs of Finland, 2022), as shown in Figure 1. Finland aims to reach 3.2% of GDP for defence expenditure by 2030. Still, this evolution falls far short of NATO's commitment at the Hague summit of Allies to increase defence investment to 5% of GDP annually by 2035, but Finland could reach the minimum target of 3.5% of GDP for defence requirements by 2035 (North Atlantic Treaty Organization, 2026).

Finland's role in defending European and Alliance security is crucial because of its long eastern frontline. Finland should increase its investment in the defence sector beyond NATO's minimum target of 3.5% of GDP to safeguard deterrence in the region. Finland has also made major procurements, notably the contract for 64 Lockheed Martin F-35A Lightning II multi-role fighters to replace Finland's old Hornet fleet (Finnish Air Force, 2021).

The changing Finnish security landscape is also reflected in Finnish political life. Finland closed all border crossing points on the eastern border in November 2023 because of Russia's

instrumentalisation of people at Finland's eastern border and the increased threat of hybrid operations (Ministry of the Interior & Prime Minister's Office, 2023). Most recently, in June 2026, the Finnish government decided to keep Finland's eastern border closed until further notice to protect national security and public order (Ministry of the Interior, 2026b).

This change is also reflected in the Finnish president's discourses. Finland, long known as a mediator between East and West, changed its foreign policy significantly since Russia's invasion of Ukraine, when Finland strongly condemned Russia's actions and warfare (President of the Republic of Finland, 2022). Finland's former president Niinistö's famous declaration summarises Finland's changed security landscape well: "now the masks are off, only the cold face of war is visible" (Tikkala et al., 2022).

"Since the Russian invasion of Ukraine, Finland has strengthened it's unique comprehensive security concept through innovations in the AI sector such as cutting-edge technology in unmanned systems."

Finland's preparation for crises dominated by the comprehensive security concept

Finland's expertise in crisis preparation is appreciated worldwide: in 2024, former president Niinistö, as Special Adviser to the President of the European Commission, submitted the report Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness. It proposes 80 short- and long-term recommendations for Europe's changing security landscape (Niinistö, 2024).

Finland also promotes its comprehensive security concept abroad, for example through a free online course on its principles produced by the Security Committee (Security Committee, n.d.).

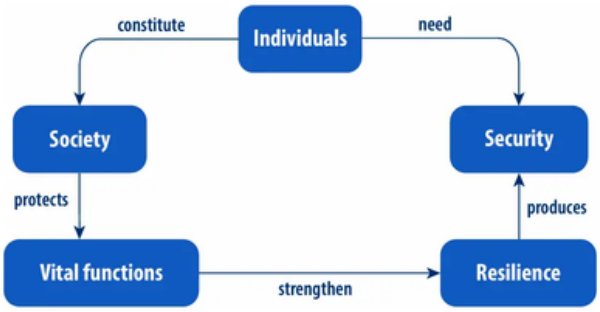


Figure 2. Finland's comprehensive security concept. Source: Security Committee (2025).

But what does the comprehensive security concept emphasise? Finland's crisis preparedness plan, the so-called comprehensive security concept, plays a key role in increasing society's resilience to crises and in better responding to hybrid threats, for example. It is based on cooperation among several actors in society, as shown in Figure 2: authorities, the business community, citizens, and organisations, sharing responsibility for society's vital functions. This concept emphasises, above all, the individual's role in responding to threats, as well as their knowledge, skills, and security-strengthening attitude, by highlighting individuals' mutual trust. Preparedness and response readiness also help society face threats and recover from them (Security Committee, 2025).

Local civic actors also play a significant role in crisis preparedness by providing advice and building citizens' capacity. A 2025 Prime Minister's Office report on local civic activity concluded that civic engagement plays a primary role in basic resilience and during crises and acute disruptions. This shows in neighbourly help in sparsely populated areas and in civil society organisations' ability to reach people (Mäenpää et al., 2025).

The Women's National Emergency Preparedness Association is a good example of how local civic actors can strengthen social preparedness. This association brings together 10 subassociations working in national defence and comprehensive security, uniting over 100,000 women by organising safety and preparedness training such as civil defence, cybersecurity, outdoor survival skills, and information influence (Naisten valmiusliitto, n.d.).

A concrete example of civil society's support for citizens is the website named 72 hours, created by the Finnish National Rescue Association and the National Emergency Supply Agency (n.d.) in cooperation with multiple NGOs. It advises households to keep enough supplies, such as food and water, to cope for at least three days. As noted earlier, Finland's defence capability is built primarily around mandatory military service for men. However, women have also been able to complete their military service since 1995 (Embassy of Finland, Athens, 2017). This individual's contribution to societal resilience is a concrete example of how Finland's comprehensive security concept functions.

Society's central role in comprehensive security was also visible in September 2026, when a massive civil defence exercise, Suojaan 2026, was organised in Kuopio. It regrouped over 2,000 people from different sectors, such as public authorities, NGOs, the business sector, and educational institutions, to test how a large population can be protected in exceptional circumstances and how emergency communication, cooperation and leadership can be improved. This exercise reinforced that Finnish security is built on cooperation among societal actors (Security Committee, 2026).



Picture 1. King Frederik X and Queen Mary of Denmark visiting Merihaka civil defence shelter. Source: City of Helsinki (2025). Photo: Sakari Röyskö.

The massive exercise and its large shelter network buttress Finland's global reputation for civil defence. Finland has over 50,500 civil defence shelters that can protect over 4.8 million people (Ministry of the Interior, 2023). As Picture 1 shows, these shelters are often shown to visiting heads of state.

Strong artificial intelligence readiness among Finnish society and its characteristics

Finland is ranked among the most advanced states globally in AI readiness. According to Eurostat (2026), Finland's SMEs have the

highest digital intensity in business among member states, and Finland has the highest percentage (79.2%) of all member states for businesses buying cloud computing services in 2025. Finland also ranks second, after Denmark, in business use of AI (37.8%) (Eurostat, 2026).

Finland's success in AI adoption stems from the widespread use of AI technologies across Finnish society, a strong government model based on predictable principles, and strong ICT expertise and innovation capacity (AI Finland & Business Finland, 2026).



Figure 3. Government AI Readiness Index 2025. Source: AI Finland & Business Finland (2026).

As Figure 3 indicates, the United States leads AI readiness worldwide, leaving Finland and Western Europe behind, especially in safety and security, compute capacity and AI sector maturity. According to the Oxford Insights report (Iida et al., 2026), China ranks 8th in state, public sector, and society capability for AI readiness, with strengths in policy vision, governance principles, and safety and security. Finland ranks 18th, scoring well in data quality, e-government delivery and especially societal transition (90.67/100), compared with the two superpowers, the United States and China, both of which score just above 50/100 (Iida et al., 2026).

One reason for Finland's strong position in AI readiness can be its first place in the 2023 Digibarometer, which measures the degree of digitalisation in societies. Finland has strengthened its digitalisation across businesses, citizens and the public sector compared with previous years. Finland is among the world leaders in many sectors, especially in citizens' digital skills and the number of mobile and fixed broadband connections (Ali-Yrkkö et al., 2023). A good example of leveraging Finland's citizens' digital skills is the VBS3 video game-style war simulator, used to train conscripts by providing realistic scenarios for practising military skills (Roslander, 2021).

Artificial intelligence, defence and social resilience

An early example of Finland's embrace of AI is Finland's Age of Artificial Intelligence (Steering Group of the Artificial Intelligence Programme, 2017), a report published by the Ministry of Economic Affairs and Employment. The report recognises the advantages of using AI in the security sector to better detect threats, increase society's preparedness, and ensure society's capacity for quick recovery, but it also stresses that individuals' privacy and protection must be guaranteed. In addition, this publication highlights Finland's strong starting position as a technology multiskilled actor to become an expert at adapting AI in the defence sector (Steering Group of the Artificial Intelligence Programme, 2017).

In November 2025, the Finnish Defence Forces introduced a data and AI strategy outlining how

AI and data can support decision-making, development, learning and operations in the long term, with the aim of making AI and data-driven management a seamless part of decision-making at all levels. Ideally, data is treated as a strategic resource to gain an advantage in administration and operational action, freeing resources for the Finnish Defence Forces' core task (Pääesikunta, 2025).

As Major General Samu Nurmi highlights, the modern battlefield extends beyond land, air and sea to include cyberspace and the information environment, and data has become a key resource rather than a mere tool (Finnish Defence Forces, 2025). The Finnish Defence Forces therefore sees data and AI as central tools for improving military performance through unmanned systems such as drones, and as essential for filtering, analysing, and combining information (Finnish Defence Forces, 2025).

Finland's AI readiness is also reflected in its defence innovation sector. As the war in Ukraine has shifted the battlefield towards unmanned systems, many Finnish companies have begun producing drones. For example, Patria, a major Finnish defence company, began cooperating with the AI start-up NestAI to produce AI-enabled unmanned aerial systems for European defence markets (Patria, 2026). Start-ups such as NestAI and Kova Labs aim to increase European defence autonomy and sovereignty. Kova Labs develops drone technology with GNSS-free navigation and obstacle avoidance for complex, contested terrain (Kova Labs, n.d.). NestAI focuses on developing a modular platform for defence systems to gain sovereign control (NestAI, n.d.).

As noted earlier in the chapter, Finland has recognised the multiple advantages of AI in increasing societal resilience, such as combating cyber threats, supporting decision-making, and helping establish situational awareness. Finnish society is still approaching the AI revolution with caution. For example, Finnish security authorities used AI for the first time as a target in the national cyber exercise (KYHA) in September 2026 in Jyväskylä, providing valuable information on the consequences of an attack on an AI service (Ministry of Transport and Communications, 2026).

Conclusion

Russia's 2022 invasion of Ukraine pushed Finland to renew its Security Strategy for Society in January 2025 to counter hybrid threats. Finland's unique comprehensive security concept is a key factor in establishing greater resilience in Finnish society. It rests on shared responsibility among authorities, businesses, citizens and organisations, with particular emphasis on the individual.

Finnish civil society plays a crucial role in preparing citizens for crises through online advice such as the 72 hours website, large civil defence exercises organised with the authorities, and voluntary preparedness training.

Finland also has strong AI readiness, reflected in SMEs' digital intensity and businesses' high adoption of AI. In answer to the research question, this readiness can be seen especially in the defence sector's start-ups like NestAI and Kova Labs, whose technology strengthens European defence autonomy and resilience against crises.

Beyond defence companies, the Finnish government has also recognised AI's advantages, for example in detecting threats, supporting decision-making, and helping establish situational awareness to increase societal resilience. The Finnish Defence Forces' 2025 data and AI strategy aims to make AI and data-driven management a seamless part of decision-making at all levels.

References

AI Finland & Business Finland. (2026). AI in Finnish business 2026. /api/wp-media/2026/04/AI-in-Finnish-Business-2026.pdf

Ali-Yrkkö, J., Kässi, O., Pajarinen, M., & Rouvinen, P. (2023). Digibarometri 2023: Data, tekoäly ja talouskasvu [Digibarometer 2023: Data, artificial intelligence and economic growth]. Taloustieto Oy. https://www.etla.fi/en/publications/other-publications/digibarometri-2023-data-tekoaly-ja-talouskasvu/

Army Command Finland. (2019, February 8). Finnish liability for military service – the bedrock of our defence for 100 years. https://maavoimat.fi/-/suomalainen-asevelvollisuus-puolustuksemme-perusta-100-vuotta?languageId=en_US

City of Helsinki. (2025). Helsinki Mayor hosts Danish royalty at City Hall. https://www.hel.fi/en/news/helsinki-mayor-hosts-danish-royalty-at-city-hall

Embassy of Finland, Athens. (2017, June 16). Naisten vapaaehtoinen asepalvelus [Women's voluntary military service]. https://finlandabroad.fi/web/grc/ajankohtaista/-/asset_publisher/TV8iYvdcF3tq/content/naisten-vapaaehtoinen-asepalvelus/384951

European Centre of Excellence for Countering Hybrid Threats. (n.d.). Establishment. https://www.hybridcoe.fi/establishment/

Eurostat. (2026). Digitalisation in Europe – 2026 edition. https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2026

Finnish Air Force. (2021, December 10). The Lockheed Martin F-35A Lightning II is Finland's next multi-role fighter. https://ilmavoimat.fi/-/lockheed-martin-f-35a-lightning-ii-on-suomen-seuraava-monitoimihavittaja?languageId=en_US

Finnish Defence Forces. (2025, November 27). Puolustusvoimien data- ja tekoälystrategia on julkaistu [The Finnish Defence Forces' data and AI strategy has been published]. https://puolustusvoimat.fi/-/puolustusvoimien-data-ja-tekoalystrategia-on-julkaistu

Finnish National Rescue Association & National Emergency Supply Agency. (n.d.). 72 hours – could you cope on your own? https://72tuntia.fi/en/#varaudu

Iida, K., Rahim, S., Hutber, C., Grau, G., Moss, C., & Douglas, O. (2026). Government AI readiness index 2025. Oxford Insights. /api/wp-media/2026/06/LATEST-GAIRI-Report-2025.pdf

Kova Labs. (n.d.). Kova Labs is an advanced engineering lab building the autonomous land force. https://kovahq.com/

Kyllönen, K.-M. (2025). Redefining national identity through security discourse: Finland's transition from military non-alignment to active defence cooperation. Cooperation and Conflict, 60(4), 702–726. https://doi.org/10.1177/00108367251377603

Mäenpää, P., Faehnle, M., Grönlund, H., Pitkänen, K., Alanko, L., & Sarkia, K. (2025). Reaction speed, local information and care: Local civic activity strengthens society's long-term resilience and crises preparedness (Publications of the Government's analysis, assessment and research activities 2025:2). Prime Minister's Office. https://urn.fi/URN:ISBN:978-952-383-340-1

Ministry for Foreign Affairs of Finland. (n.d.). Finland's membership in NATO. Finland Abroad. https://finlandabroad.fi/web/nato/finlands-membership-in-nato

Ministry for Foreign Affairs of Finland. (2022, May 17). Finland declares its interest to accede to NATO. https://um.fi/current-affairs/-/asset_publisher/gc654PySnjTX/content/suomi-ilmoittaa-kiinnostuksensa-liittya-natoon

Ministry of Defence. (n.d.). Defence budget. https://defmin.fi/en/ministry-of-defence/economy-and-activities/defence-budget

Ministry of Defence. (2025, January 16). Finland's comprehensive security reinforced through new security strategy for society. Finnish Government. https://valtioneuvosto.fi/en/-/236553176/finland-s-comprehensive-security-reinforced-through-new-security-strategy-for-society

Ministry of the Interior. (2023, February 9). Finland has civil defence shelters for about 4.8 million people. Finnish Government. https://valtioneuvosto.fi/-/1410869/suomessa-on-vaestonsuojapaikkoja-noin-4-8-miljoonalle-ihmiselle?languageId=en_US

Ministry of the Interior. (2026a, March 20). EU provide Finland with EUR 17 million for surveillance of the eastern border and Gulf of Finland. Finnish Government. https://valtioneuvosto.fi/-/1410869/eu-tukee-valvontajarjestelmien-hankintaa-suomen-itarajalle-ja-suomenlahdelle-17-miljoonalla-eurolla?languageId=en_US

Ministry of the Interior. (2026b, June 4). Finland's eastern border to remain closed until further notice. https://intermin.fi/-/itaraja-pysyy-suljettuna-toistaiseksi?languageId=en_US

Ministry of the Interior & Prime Minister's Office. (2023, November 28). Finland's entire eastern border to be closed. Finnish Government. https://valtioneuvosto.fi/en/-/1410869/finland-s-entire-eastern-border-to-be-closed

Ministry of Transport and Communications. (2026, September 28). Tekoäly ensimmäistä kertaa hyökkäyksen kohteena kansallisessa kyberharjoituksessa [AI targeted by an attack for the first time in a national cyber exercise]. Finnish Government. https://valtioneuvosto.fi/-/1410829/tekoaly-ensimmaista-kertaa-hyokkayksen-kohteena-kansallisessa-kyberharjoituksessa

Naisten valmiusliitto. (n.d.). Kaiken varalta! [Prepared for anything!]. https://naistenvalmiusliitto.fi/

NestAI. (n.d.). Adaptive intelligence for Europe's security. https://www.nestai.com/

Niinistö, S. (2024). Safer together: Strengthening Europe's civilian and military preparedness and readiness. European Commission. https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

North Atlantic Treaty Organization. (2026, June 29). Defence investment and NATO's 5% commitment. https://www.nato.int/en/what-we-do/introduction-to-nato/defence-expenditures-and-natos-5-commitment

Pääesikunta. (2025). Puolustusvoimien data- ja tekoälystrategia [Data and AI strategy of the Finnish Defence Forces]. Finnish Defence Forces. https://puolustusvoimat.fi/documents/1948673/2273743/Puolustusvoimien_Data_ja_teko%C3%A4lystrategia_JULK.pdf/96190125-e811-e08b-dcbc-660f67a94a81/Puolustusvoimien_Data_ja_teko%C3%A4lystrategia_JULK.pdf?t=1764246963044

Patria. (2026, May 25). Patria and NestAI partner on AI-enabled unmanned aerial systems for European defence. https://www.patriagroup.com/newsroom/news/2026/patria-and-nestai-partner-on-ai-enabled-unmanned-aerial-systems-for-european-defence

Pesu, M. (2023). NATO in the North: The emerging division of labour in Northern European security (FIIA Briefing Paper No. 370). Finnish Institute of International Affairs. /api/wp-media/2023/09/bp370_nato-in-the-north.pdf

President of the Republic of Finland. (2022, February 24). President Niinistö: Finland strongly condemns Russia's actions and warfare. https://www.presidentti.fi/niinisto/en/news/president-niinisto-finland-strongly-condemns-russias-actions-and-warfare/index.html

Roslander, E. (2021, January 22). Sotasimulaattori tuo taistelukoulutuksen ruudulle [War simulator brings combat training to the screen]. Ruotuväki. https://ruotuvaki.fi/-/sotasimulaattori-tuo-taistelukoulutuksen-ruudulle

Salonius-Pasternak, C., & Limnéll, J. (2015). Preparing Finland for hybrid warfare: Social vulnerabilities and the threat of military force (FIIA Comment 6/2015). Finnish Institute of International Affairs. /api/wp-media/2017/01/comment6_2015eng.pdf

Security Committee. (n.d.). Online course on comprehensive security now available in English at eOppiva. https://turvallisuuskomitea.fi/en/online-course-on-comprehensive-security-now-available-in-english-at-eoppiva/

Security Committee. (2025). Security strategy for society [Government resolution]. Finnish Government. https://julkaisut.valtioneuvosto.fi/server/api/core/bitstreams/aff0ba13-4037-43e8-8b85-e138215ce3ac/content

Security Committee. (2026). Suojaan 2026 toi yhteiskunnan turvallisuusstrategian käytäntöön Kuopiossa [Suojaan 2026 put the Security Strategy for Society into practice in Kuopio]. https://turvallisuuskomitea.fi/suojaan-2026-toi-yhteiskunnan-turvallisuusstrategian-kaytantoon-kuopiossa/

Steering Group of the Artificial Intelligence Programme. (2017). Finland's age of artificial intelligence: Turning Finland into a leading country in the application of artificial intelligence. Objective and recommendations for measures. Ministry of Economic Affairs and Employment of Finland. https://tem.fi/en/publication?pubid=URN:ISBN:978-952-327-290-3

Tikkala, H., Harjumaa, M., Orjala, A., Tolkki, K., & Hakahuhta, A. (2022, February 24). Presidentti Sauli Niinistö: "Nyt naamiot on riisuttu, vain sodan kylmät kasvot näkyvät" – näin Suomen johto tuomitsi Venäjän hyökkäyksen [President Sauli Niinistö: "Now the masks are off, only the cold face of war is visible" – how Finland's leadership condemned Russia's attack]. Yle. https://yle.fi/a/3-12331829

“

Europe has spent years strengthening sovereignty over its data. The next challenge lies beneath it.

— **Cliona Hennessy, Route Sovereignty**

ARTIFICIAL INTELLIGENCE & CYBERSECURITY



Biometrics, Surveillance and Control at the Border.

Laura Nicole Binetti

About the Article

"Biometric border management is therefore expanding before the surrounding legal framework is complete."

About the Author

Laura Nicole Binetti is an Italian Master's student in Global Security and Strategy at the Brussels School of Governance. She holds a BA in Political Science and International Relations from the University of Milan, with a minor in Law, Integration and Markets and a thesis on the Mattei Plan for Africa. Her current research examines how NATO can lawfully deploy AI enabled uncrewed maritime systems in the Baltic Sea, combining legal analysis with qualitative interviews.

Schengen Mobility in the Age of the EES

On 10 April 2026, the European Union's Entry/Exit System (EES) became fully operational across the Schengen area, replacing passport stamps with fingerprints and facial scans (Wahl, 2026). Phased in from 12 October 2025, the EES is the most extensive biometric border system the EU has introduced so far. It records the entry, exit and biometric data of third-country nationals subject to the system who cross an external Schengen border for a short stay (Council of the European Union, 2025). However, the EES is not just a technical upgrade. Its introduction comes at a time when the EU is also trying to regulate the growing use of artificial intelligence through the AI Act, which treats biometric identification as a particularly sensitive area (European Commission, 2026a).

This creates an important tension. The EU presents itself as a global leader in regulating digital technologies while protecting fundamental rights. At the same time, it operates one of the world's largest biometric border systems. The Schengen area's foundational promise (that of free movement without systematic identity checks) was built for a paper-based world of passport stamps and visual inspection. Today, this system has to coexist with facial recognition, centralised biometric databases and interconnected information systems that can also be accessed for purposes of law enforcement.

The question is also timely. The EES became fully operational in April 2026, and the Pact on Migration and Asylum has applied since 12 June 2026 (Council of the European Union, 2026). ETIAS is not yet in operation (European Commission, 2025), and the AI Act's high-risk rules apply later. Biometric border management is therefore expanding before the surrounding legal framework is complete.

This paper asks whether these two developments can coexist: can the EU use biometric technologies at its external borders without weakening the promise of free movement at the heart of the Schengen area?

Function creep is the gradual widening of the use of a system beyond the purpose for which it was originally intended, particularly when this risks privacy invasion or unauthorised surveillance.

Schengen, Borders and Biometrics

The Schengen area is often described as a "borderless Europe", but in practice the system is more complex. Border controls between member states were removed, while controls at the common external borders were strengthened and increasingly managed at the European level (European Parliament, 2025).

As internal border controls disappeared, member states invested more in managing the external borders, and biometric identification became increasingly important. EU biometric border systems mainly use two types of biometric data: facial images and fingerprints, collected from third-country nationals when they enter or leave the Schengen area. These systems are part of the EU's broader "smart borders" policy, developed to make external border checks faster, more automated and less dependent on

manual document checks (European Commission, 2026, August 10).

The EES is the clearest example of this approach. Instead of simply stamping a passport, the system creates an electronic file for each third-country national it covers. Figure 1 shows how this works at the border. At a first crossing, the traveller's travel document is scanned, and a facial image and fingerprints are taken; at later crossings, these data are verified against the file. For visa holders, the data are also checked against the Visa Information System (VIS). Each entry and exit is recorded, and the system automatically calculates whether the traveller has exceeded the permitted 90-day stay in any 180-day period (Council of the European Union, 2025; European Union, 2017).

The system was introduced gradually over six months. At least ten per cent of estimated border crossings were covered after the first month, with all eligible travellers registered by April 2026. A gradual rollout was chosen because introducing the system everywhere at the same time could have created problems for the system and passenger flows (European Union, 2025).

What used to be a simple border check now involves collecting and storing personal data in a centralised EU database. The scale is considerable: in its first six months, the EES registered over 66 million entries and exits and 32,000 refusals of entry (European Commission, 2026b). These figures count crossings, not travellers, and cover a phased rollout, so they are not an annual total. This change raises important legal and political questions, which the rest of this paper will examine.

The first months of the EES have not been without problems. Some airports reported long queues after the full launch, and nine member states asked the EU to extend a temporary measure allowing border guards to suspend biometric checks during busy periods (Banks, 2026).

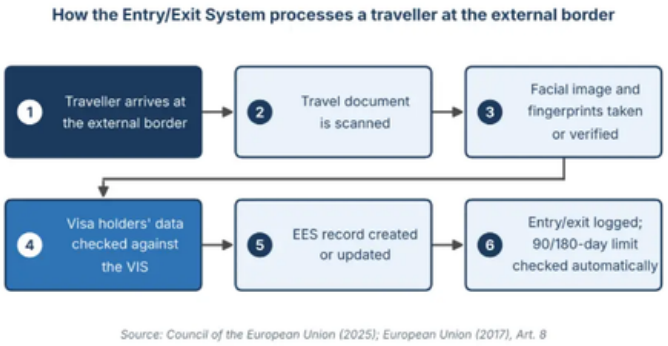


Figure 1. How the Entry/Exit System processes a traveller at the external border.

The Legal Framework

The EU did not build the EES in a legal vacuum. Since 2024, it has had in place the AI Act, the world's first comprehensive attempt to regulate artificial intelligence through a general and cross-sectoral law rather than through voluntary guidelines (European Commission, 2026a). The Act follows a risk-based approach, dividing AI systems into four levels of risk: unacceptable, high, limited and minimal (Figure 2). Some uses of biometric identification are considered particularly sensitive and are therefore either prohibited or subject to stricter rules.

Article 5 of the AI Act prohibits certain uses of biometric identification. In particular, it generally prohibits real-time remote biometric identification in public spaces for law enforcement purposes. However, three exceptions are allowed: searching for victims of abduction, trafficking or sexual exploitation and for missing persons;

preventing a specific and imminent threat to life or a terrorist attack; and identifying or locating suspects of certain serious crimes. These exceptions concern law enforcement use in public spaces under the AI Act and are not functions of the EES. Together, the restrictions show that the EU considers real-time biometric identification particularly sensitive.

The EES itself is not a high-risk AI system, but mainly a large-scale information system. Instead, the AI Act classifies specific AI tools used in migration, asylum and border control as high-risk. Annex III includes systems used to assess risks or to detect, recognise or identify individuals, while systems used only to verify travel documents are excluded. When these high-risk AI tools are used at the border, they must follow specific requirements on human oversight, accuracy, record-keeping and assessment.

"The open question is whether this legal structure is enough to contain the practical risks the EES and its companion systems create."

However, these rules do not all apply immediately. The Digital Omnibus (Regulation (EU) 2026/1744), in force since 27 July 2026, postponed the main obligations for high-risk AI systems listed in Annex III until 2 December 2027 (European Union, 2026). There is an even longer transition period for AI systems that are part of large-scale EU border databases, including the EES. Under Article 111 of the AI Act, systems introduced before 2 August 2027 have until 31 December 2030 to comply (European Union, 2024; Vavoula, 2024). Figure 2 shows where border biometric tools sit in this classification and which deadlines apply to them. The border infrastructure is therefore already operating while some of the AI Act rules applying to its AI components will only become fully applicable later.

The EES is also subject to data protection oversight. The European Data Protection Supervisor (EDPS) works with national data protection authorities through the Coordinated Supervision Committee to monitor the system at both EU and national levels (European Data Protection Supervisor, 2025). The EDPS has stressed that personal data protection is a fundamental right and fully applies to the EES.

Taken together, the AI Act's risk classification and the EDPS's supervisory mandate show that EU law already treats biometric border tools as a distinct category requiring heightened scrutiny. The open question is whether this legal structure is enough to contain the practical risks the EES and its companion systems create. This is the subject of the next section.

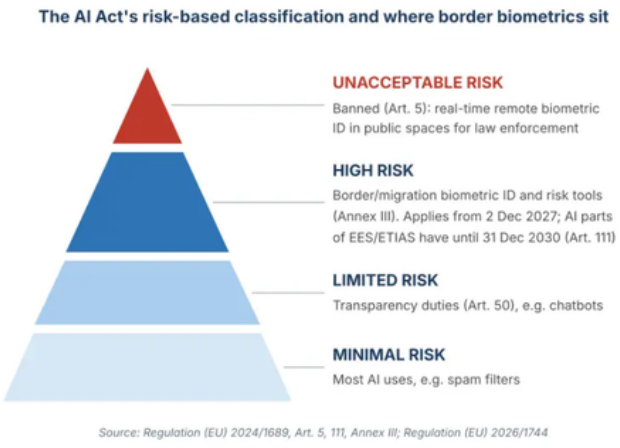


Figure 2. The AI Act's risk-based classification and where border biometrics sit.

Main Concerns

Three main concerns appear in the literature on EU biometric border systems: function creep, the risks created by interoperability and the impact of biometric controls on the idea of open mobility within Schengen.

Function creep means that data collected for one purpose is later used for another. A common example is Eurodac, the EU fingerprint database originally created to determine which member state is responsible for an asylum claim under the Dublin Regulation. It was later opened to police and law enforcement authorities for investigative purposes (Tsormpatzoudi et al., 2015). This is concerning because it challenges the principle of purpose limitation, a core rule of EU data protection law: personal data should be collected for specified purposes and not used in ways that are incompatible with them. It also affects the rights to private life and to the protection of personal data in Articles 7 and 8 of the EU Charter of Fundamental Rights (European Union, 2012). Each new use of the data is an additional interference with these rights, and it must be necessary and proportionate (European Union, 2012, Art. 52(1)). The risk is greater for third-country nationals, who provided their data as travellers or asylum seekers, not as suspects, and who have little practical ability to object. Once large amounts of biometric data are stored in a centralised system, pressure to use them for purposes beyond those for which they were collected may grow.

The second concern is interoperability. The EES is connected to a wider network of EU information systems. These include the Visa Information System (VIS), the Schengen Information System (SIS), the European Travel Information and Authorisation System (ETIAS), which is not yet in operation (European Commission, 2025), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN). Regulations (EU) 2019/817 and 2019/818 support this interoperability through tools such as a shared search portal and a common identity repository (European Union, 2019a, 2019b). Statewatch argues that linking these systems is creating a de facto centralised EU database containing biometric and personal data on non-EU nationals (Bunyan, 2018). The EU Fundamental Rights Agency has also raised concerns about the position of people whose data is stored in these systems, particularly migrants and asylum seekers. They may find it difficult to understand how their data is being used, correct inaccurate information or exercise their rights of access (European Union Agency for Fundamental Rights, 2018). Interoperability can make border systems more efficient, but it also allows identity and biometric data to be searched across different systems, within the access rules established by EU law. This can also increase the possibilities for profiling and algorithmic risk assessment (Derave et al., 2022; Vavoula, 2021).

The third concern is how biometric controls can change the experience of crossing a Schengen border. Providing fingerprints and a facial image is different from simply having a passport checked and stamped by a border guard. Even when privacy rules are respected, the growing use of biometric registration can make border crossings feel more controlled and less open. This creates a tension with the idea of Schengen as an area of free and easy movement.

Legal and Political Implications

These concerns are not only technical issues that can be solved by improving how the system works. They also raise important legal and political questions about individual rights and trust in public institutions.

From a legal perspective, biometric border systems can affect several rights protected by the EU Charter of Fundamental Rights, including privacy, personal data protection, non-discrimination and the right to an effective remedy. The Open Society Foundations raised similar concerns when the EES was first proposed in 2013. It argued that creating such a system mainly to identify "overstayers" could be disproportionate, especially given its limited ability to actually locate them (Butler, 2013). Now that the EES is fully operational, its impact and proportionality can be assessed in practice rather than only in theory.

Politically, the issue also matters for the EU's credibility as a setter of global standards. During the AI Act era, the EU has presented itself as a model for regulating digital technologies while protecting fundamental rights. However, Vavoula argues that important gaps remain in how the AI Act applies to EU border systems. For example, anonymised statistical data used within the interoperability system falls outside EU data protection law (Vavoula, 2024). This could raise doubts about whether the EU applies the same standards to its own systems that it expects from other actors.

Another point worth considering is whether the EU has benefited from the system. The Commission reports 32,000 refusals of entry in the first six months (European Commission, 2026b) and, by 10 April 2026, over 700 people identified as posing a security risk (European Commission, 2026c). These figures show that the system is being used, but a refusal is not the same as a criminal being stopped, and they say nothing about proportionality. No independent evaluation of cost savings or security gains appears to be available yet, while reported difficulties include long queues at some airports (Banks, 2026).

Possible Safeguards

These concerns do not mean that biometric border management should be abandoned, but they show the importance of having strong safeguards in place.

First, the principle of purpose limitation needs to be strictly applied. Data collected by the EES to manage entries of short-stay and exits should not be used for broader law enforcement purposes without a clear legal basis and a specific justification. The development of Eurodac shows how biometric data collected for one purpose can later be used for others, and critics have raised similar concerns about the EU's wider interoperability system (Tsormpatzoudi et al., 2015; Bunyan, 2018).

Second, oversight bodies need enough resources to effectively monitor a system as large as the EES. The EDPS and the Coordinated Supervision Committee already have a formal role in supervising the system (European Data Protection Supervisor, 2025). Strong oversight is especially important during the first years of the EES, as problems can become more difficult to address once the system is fully integrated into border operations across 29 countries.

Third, greater transparency towards travellers is needed. Data protection rights are only effective if people understand how their personal and biometric data is used and know how to exercise their rights. The EDPS has also stressed the importance of transparency and of informing travellers about their rights. However, this information should be provided in a clear and consistent way across all Schengen border crossing points.

None of these safeguards requires abandoning biometric border management altogether. Instead, they require the EU to actively enforce the rules and oversight mechanisms that are already in place, including the AI Act and the role of the EDPS.

Conclusion

The Entry/Exit System's transition from proposal to fully operational infrastructure marks a genuine turning point in how the EU manages its external border, and by extension, in what Schengen's promise of free movement actually means in practice. There is a clear tension between the growing use of biometric controls for security purposes and the idea of Schengen as an open area of free movement. The fact that the AI Act recognises the risks of biometric technologies does not remove this tension.

The main risks identified in this paper show that the expansion of biometric border management is not only a question of efficiency or security. It also raises questions about how personal data may be used over time, particularly as EU information systems become increasingly interconnected. Early figures suggest that the system is producing results, but its benefits have not yet been independently assessed.

For Schengen to remain an area that is both open and respectful of rights, biometric border systems need strong safeguards. Purpose limitation must be respected, oversight bodies need sufficient resources, and greater transparency towards travellers is necessary. These safeguards must be applied continuously in practice, rather than simply included in EU legislation.

References

Banks, M. (2026, August 10). EU could extend flexibility on EES border checks amid fears of further travel disruption. Travel Tomorrow. https://traveltomorrow.com/eu-could-extend-flexibility-on-ees-border-checks-amid-fears-of-further-travel-disruption/

Bunyan, T. (2018). Briefing: The interoperability of Justice and Home Affairs databases. Statewatch. https://statewatch.org/analyses/2018/briefing-the-interoperability-of-justice-and-home-affairs-databases/

Butler, I. (2013, April 23). No good reason for a Schengen entry/exit system. Open Society Foundations. https://www.opensocietyfoundations.org/voices/no-good-reason-schengen-entryexit-system

Council of the European Union. (2026). Pact on migration and asylum. https://www.consilium.europa.eu/en/policies/eu-migration-policy/eu-migration-asylum-reform-pact/

Council of the European Union. (2025, October 11). With start of operation of new EES border control system the EU will strengthen border security and increase efficiency for travellers [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2025/10/11/with-start-of-operation-of-new-ees-border-control-system-the-eu-will-strengthen-border-security-and-increase-efficiency-for-travellers/

Derave, C., Genicot, N., & Hetmanska, N. (2022). The risks of trustworthy artificial intelligence: The case of the European Travel Information and Authorisation System. European Journal of Risk Regulation, 13(3), 389–420. https://doi.org/10.1017/err.2022.5

European Commission. (2026, August 10). Entry/Exit System (EES). https://home-affairs.ec.europa.eu/policies/schengen/smart-borders/entry-exit-system_en

European Commission. (2025, October 6). European Travel Information and Authorisation System (ETIAS). https://home-affairs.ec.europa.eu/policies/schengen/smart-borders/european-travel-information-authorisation-system_en

European Commission. (2026a, August 3). AI Act. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Commission. (2026b, May 18). Commission report shows Schengen area continues to be resilient and ready for future challenges [News]. https://luxembourg.representation.ec.europa.eu/actualites-et-evenements/actualites/commission-report-shows-schengen-area-continues-be-resilient-and-ready-future-challenges-2026-05-18_en

European Commission. (2026c, April 10). Entry/Exit System (EES) is fully operational [News]. https://home-affairs.ec.europa.eu/news/entryexit-system-ees-fully-operational-2026-04-10_en

European Data Protection Supervisor. (2025, October 24). Supervising the entry into operations of the Entry/Exit System [Press release]. https://www.edps.europa.eu/system/files/2025-10/2025_10_Supervising_EU_Entry_Exit_System_EN.pdf

European Union. (2012). Charter of Fundamental Rights of the European Union. Official Journal of the European Union, C 326, 391–407. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

European Parliament. (2025). Free movement of persons. Fact Sheets on the European Union. https://www.europarl.europa.eu/factsheets/en/sheet/147/free-movement-of-persons

European Union. (2017). Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011. Official Journal of the European Union, L 327, 20–82. https://eur-lex.europa.eu/eli/reg/2017/2226/oj

European Union. (2019a). Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 establishing a framework for interoperability between EU information systems in the field of borders and visa. Official Journal of the European Union, L 135, 27–84. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0817

European Union. (2019b). Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration. Official Journal of the European Union, L 135, 85–135. https://eur-lex.europa.eu/eli/reg/2019/818/oj

European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

European Union. (2025). Regulation (EU) 2025/1534 of the European Parliament and of the Council of 18 July 2025 on temporary derogations from certain provisions of Regulations (EU) 2017/2226 and (EU) 2016/399 as regards the progressive start of operations of the Entry/Exit System. Official Journal of the European Union, L 2025/1534. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R1534

European Union. (2026). Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). Official Journal of the European Union, L 2026/1744. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1744

European Union Agency for Fundamental Rights. (2018). Under watchful eyes: Biometrics, EU IT systems and fundamental rights. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/abefeb05-387b-11e8-b5fe-01aa75ed71a1/language-en

Tsormpatzoudi, P., Dimitrova, D., Schroers, J., & Kindt, E. (2015). Privacy by design: The case of automated border control. In Privacy and identity management for the future internet in the age of globalisation (Vol. 457, pp. 139–152). Springer. https://doi.org/10.1007/978-3-319-18621-4_10

Vavoula, N. (2021). Artificial intelligence (AI) at Schengen borders: Automated processing, algorithmic profiling and facial recognition in the era of techno-solutionism. European Journal of Migration and Law, 23(4), 457–484. https://doi.org/10.1163/15718166-12340114

Vavoula, N. (2024, December 13). Regulating AI at Europe's borders: Where the AI Act falls short. Verfassungsblog. https://doi.org/10.59704/10a27137a898fa42

Wahl, T. (2026, April 15). Entry/Exit System (EES) fully operational since 10 April 2026. eucrim. https://eucrim.eu/news/entryexit-system-ees-fully-operational-since-10-april-2026/

Join EPIS

Become part of the EPIS Think Tank

EPIS is both a network and a think tank in foreign and security policy. The EPIS Network connects students and graduates, supporting their careers. The EPIS Think Tank produces publications in various formats on different regions and topics. Together, they form EPIS—where you can join passively as a network member or actively contribute to publications. Interested? Apply now for an onboarding meeting & follow us on social media!

Want to author the next EPIS Report?

Apply for FASP now and contribute to one of our Thematic Report Groups – from Artificial Intelligence & Cybersecurity and Security Policy & Defence to Human Rights & Humanitarian Aid and Climate Policy & Environment.

epis-thinktank.com

Contact: board.external@epis-thinktank.com

ARTIFICIAL INTELLIGENCE & CYBERSECURITY



The Accountability Paradox of Commercial Spyware: the NSO Group Case

Giulia Rossi

About the Article

"This report examines whether accountability mechanisms are able to effectively constrain commercial spyware, or rather, they inadvertently legitimise it."

About the Author

Giulia Rossi is a International Relations student and Global Governance graduate with a strong passion for international security and information control in authoritarian regimes. Passionate about traveling and intercultural exchange, she aims to learn from as many people and contexts as possible. Her goal is to continuously broaden her perspective while contributing to a more informed and connected international community.

1.400, this is the number of WhatsApp users who had their phones hacked by the Pegasus spyware and for which Meta started a long legal battle in October 2019. The malware was able to access private data by mimicking WhatsApp's server itself through phone calls to victims with different country code prefixes such as the Kingdom of Bahrain, the United Arab Emirates and Mexico. Consequently, Pegasus was able to take full control of the target's smartphones and all their stored information (Silberman, 2024). The NSO Group, an Israeli firm and developer of the spyware, continued to cause multiple system breaches throughout the six-year litigation process despite several court orders, with Meta's legal team alleging that the company deliberately defied the court's injunctions and demands (Simons, 2024).

This report examines whether accountability mechanisms are able to effectively constrain commercial spyware, or rather, they inadvertently legitimise it. In June 2026, Meta filed a contempt motion against NSO and, shortly after, a member of the European Parliament's spyware investigation committee was targeted with Pegasus in July 2026. The analysis uses NSO Group as a case study through a qualitative review of court filings, lobbying disclosures and academic literature. While experts have addressed this tool's capabilities and human rights implications separately, this report argues that their structural interaction, specifically how legal and regulatory responses produce a paradox of legitimisation, remains underexplored. From the Meta litigation, through the Entity list dynamics, to NSO's ties with the State of Israel, the report delves into an original argument on the governance failure of commercial spyware.

The Court Litigation and Its Governmental Shadows

On February 23, 2024, Judge Phyllis J. Hamilton ordered NSO Group to "produce information concerning the full functionality" of the spyware and any other "remote access trojan" that the company developed (Lubin, 2024), on top of the original code of Pegasus. NSO argued that Israeli law prevents them from reproducing the code out of country and disclosing sensitive production information admissible at trial (Simons, 2024). However, leaked files from multiple media organisations revealed that in July 2020, Israeli officials had previously physically seized documents and equipment from NSO's offices in Tel Aviv, in order to prevent the company from complying with WhatsApp's eventual requests and transferring confidential documentation without explicit governmental authorisation (Davies et al., 2024).

The whole operation was under gag order, preventing the actions from being divulged. Scott Horton, lawyer and professor at Columbia Law School, described these as "strange procedures to be taking in relation to a private entity", suggesting NSO was in fact an "integral part of the Israeli defence establishment" (Davies et al., 2024). This last point is indicative of a foreign authority shielding a supposedly independent and private firm, de facto designating it as a national strategic asset, free from judicial oversight. Ultimately, the California jury ended up awarding over $167,000,000 in punitive damages and over $400,000 in compensatory damages to Meta (Novo, 2025), an

unprecedented event for platform liability in the spyware industry.

In June 2026, the WhatsApp v. NSO Group regained public attention due to Meta accusing NSO of continuously violating the permanent injunction that banned them from operating on the network. The evidence of these illegal actions was 23 WhatsApp accounts and 34 groups identified as "test groups". Meta security engineer Andrew Blaich identified the clusters in at least 13 countries, with names explicitly referencing test operations in Sub-Saharan Africa, the Middle East and Central America (Mitra, 2026). According to the filing, through one-click links, NSO Group was capable of accessing classified material (Mitra, 2026).

The Entity List is a US Commerce Department blacklist of foreign entities seen as threats to national security or foreign policy. Once listed, US firms need a licence to export technology to them.

These new accusations are only adding to the multiple controversies that the Israeli developer had to face before and during the many years of trial against WhatsApp. For instance, in a 2017 inquiry by The New York Times, it was reported that Mexico acquired Pegasus to investigate criminals and terrorists. Despite the initial claim, the targets turned out to mainly be HR lawyers, correspondents and anti-corruption activists (Silberman, 2024).

Lobbying as a response to blacklisting

The global reach of NSO's operations, combined with its demonstrated contempt for US court orders, prompted a regulatory response from Washington. In November 2021, under Biden's administration, the US Commerce Department added NSO Group and another Israeli commercial spyware company, Candiru (Lubin, 2024), to its Entity List, a federal blacklist which prohibits the exchange of American technologies. The official governmental statement explained this choice as proof of the administration's "efforts to put human rights at the centre of U.S. foreign policy, including by working to stem the proliferation of digital tools

"The case can be made for a foreign authority shielding a supposedly independent and private firm, de facto designating it as a national strategic asset, free from judicial oversight."

used for repression." The press release further indicates that the NSO Group "enabled foreign governments to conduct transnational repression [...] Such practices threaten the rules-based international order." (U.S. Department of Commerce, 2021).

From that moment on, an aggressive lobbying campaign began in order to remove NSO from the Entity List, principally since the presidential change. In 2025, Caroline Glick, a key advisor to Israeli prime minister Benjamin Netanyahu, was reported by Tel Aviv's media to be in the process of working with the Trump administration to lift the current sanctions (Ilnai, 2025). Moreover, in

November of the same year, the company announced a new shareholder structure, with the consequent election of David Friedman as chairman (Panagiotopoulos, 2026). During his first term, Donald Trump described Friedman as a "long-time friend and trusted adviser" (Trump, 2016) thanks to his prior service as United States ambassador to Israel. It is therefore not a secret that Friedman intends to use his diplomatic ties to help restore Pegasus' reputation amongst American investors and US officials (Panagiotopoulos, 2026).

Another key aspect of NSO's rehabilitation strategy has been the Vogel Group, a Washington-based government affairs and consulting firm with direct ties to the Republican establishment and the Trump administration. In 2025, it was listed as Israel's software company's primary lobbying contractor (U.S. House of Representatives, 2026). While NSO's previous lobbying contractors were registered under the Foreign Agents Registration Act (FARA), which mandates detailed disclosure of any meetings or acts of influence by foreign governments and political parties, the Vogel Group registered under the Lobbying Disclosure Act (LDA), a significantly less transparent instrument that requires only broad quarterly reports with no obligation to specify whether the meetings are held for commercial or diplomatic interests (Dennett, 2018). This shift from FARA to LDA, occurring precisely as Trump returned to the White House for his second term, confirms NSO Group as a direct client with a base in Israel, yet the content of that relationship remains largely shielded from public scrutiny by thoughtful design. Overall, the scale of this effort, at least $7.7 million in lobbying professionals and consultants between 2020 and 2025 (Lieber, 2025), clearly reflects something more than a private company seeking regulatory relief.

Perhaps the most revealing indicator of NSO's confidence in its political protection came in a rare interview to Israeli media dated December 2024, where NSO's co-founder Omri Lavie openly downplayed the impact of the Entity List designation: "The Americans, when they say blacklist, it sounds much more dramatic to me than it actually is. You can still do business in the United States; it is definitely not a barrier for us to sell in the US. I strongly believe that what we are doing is important and essential both for the State of Israel and for the world" (Frenkel, 2024). This declaration openly explains how a governmental regulatory tool like the Entity List has not fulfilled expectations and instead blurs the line between a private commercial enterprise and a sovereign tactical tool.

NSO's roots in Israeli State Infrastructure

Surveillance technology firms find in Israel a perfect ground to establish and flourish, making it the "Silicon Valley" of commercial spyware (Silberman, 2024). These private entities primarily recruit from MID graduates, most notably Unit 8200 alumni. The latter is a crucial asset to Israel's renowned cyber ecosystem, and each year approximately 1,000 top-notch cyber experts join the ranks of Israeli defence, industry and academia (Cohen et al., 2024). In recent years, due to the prestige of its cyber education, Unit 8200 talents have started to be more interested in the highly remunerative private sector of digital corporations like NSO, Cellebrite, Cytrox and Candiru (Ilnai, 2025).

The structural ties between NSO and the state of Israel, being intrinsically organisational, are a crucial apparatus when it comes to primary needs and protection of the country. The Ministry of Defence acquired Pegasus in 2013 and began operating with it in 2015 (Rubin, 2022). Years later, in 2022, Calcalist, Israel's leading economics newspaper, released an exclusive list of dozens of citizens and political figures who had reported having their devices hacked by Israeli police through Pegasus' malware (Ganon, 2022). The platform explained how these targets included anti-government protesters, senior parliament members, ministers and even Benjamin Netanyahu's entourage and family.

The revelation that Pegasus' zero-click spyware had been utilised by Israeli authorities for domestic law enforcement purposes caused massive turmoil in the Jewish state's society (Lubin, 2024), which, until that moment, had assumed that such tools were mostly reserved for national security purposes (Rubin, 2022). Regarding this last aspect, since Hamas' attack on the 7th of October 2023, the Israel Defence Forces have partnered with NSO Group in order to strengthen surveillance in the Gaza Strip (Blessing, 2024). In a 2025 report to the UNHRC, Francesca Albanese, Special Rapporteur on the Occupied Palestinian Territories, explains how there's evidence of the spying malware being used to target Palestinian activists, leaders, journalists and human rights defenders who speak in favour of the recognition of the genocide (Albanese, 2025). Additionally, Pegasus has also been used to monitor phones in the West Bank, with the scope of retrieving vital information on Hamas members' locations and blackmailing fragile individuals (Gray, 2025). The malware has been employed in the field of other sensitive areas for the state of Israel, such as Iran, Lebanon and Yemen (Harwell et al, 2021). When questioned on the integrity of these actions towards Arabs and Palestinians, NSO's former CEO Hulio Shalev firmly stated: "If Israel is using our tools to fight crime and terror, I would be very proud of it." (Farrow, 2022).

With this level of premises, NSO's top product has easily become an alluring tool for most regimes around the world. Following the 2007 Defence Export Controls law, Israel's Ministry of Defence is designated as the only licensed institution able to decide whether and to whom to sell the country's cyberweapons outside domestic jurisdiction (Feldstein et al., 2023). Geopolitical events directly shape export licence decisions. When Ukraine tried in 2022 to acquire Pegasus, the whole operation was quickly shut down (Feldstein et al., 2023). Israeli officials did not want to undermine relations with Russia (Ward, 2023).

Human Rights Implication of Commercial Spyware

The consequences of selling such powerful spyware abroad are not abstract, but once Pegasus reaches its designated clients, Israel has no formal mechanism to supervise how it is deployed. A cross-analysis by Forbidden Stories and Amnesty International indicated a list of fifty thousand phone numbers that were targeted by a wide variety of countries with a history of human rights abuses and citizen surveillance (Amnesty International, 2021). Such countries are Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates, which have all been identified as instigators of spying operations (De Martin, 2024). Said

victims ranged from Arab royal family members, entrepreneurs, human rights advocates, writers, and more than 600 government officials (Amnesty International, 2021). One of the most infamous cases is the assassination of Washington Post reporter Jamal Khashoggi. After the killing, investigators found that the smartphones of the Saudi journalist's close associates had previously been infected with Pegasus (De Martin, 2024).

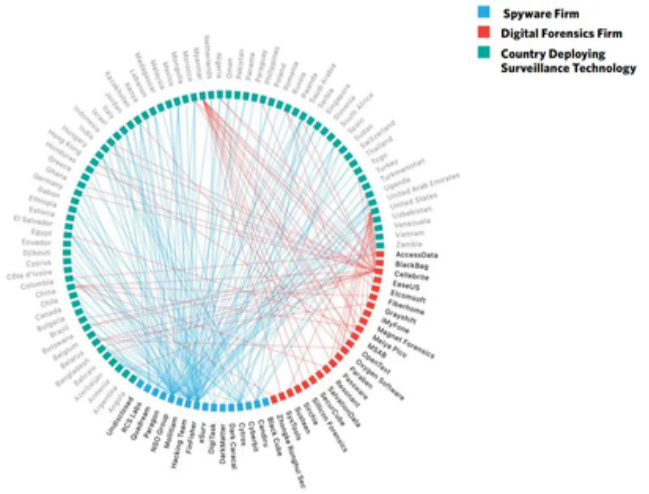


Figure 1. Key Relationships between Governments and Intrusion Technology Firms. Data source: Carnegie Endowment for International Peace (2023). Available at: https://carnegieendowment.org/features/commercial-spyware

While companies based in or connected to Israel have sold surveillance products to 56 of 74 identified governments active in the cyber trade between 2010 and 2023 (Feldstein et al., 2023), they are not the only ones in the global landscape. Major firms have rapidly joined the market, notably the Indian "BelltroX", the UAE "Crowdfense", the Italian "RCS Labs", and the French "Intellexa" (Lubin, 2024). Blacklisting companies who perpetrated infringement of human rights – like the US did with the Entity List – has proven to be ineffective.

The nature of the issue is rooted in the political economy of a sectoral market like intrusive technology (Feldstein et al., 2023), which is only destined to grow in demand. Policymakers' first objective would be to monitor the extensive exploitation of apparently lawful regulatory loopholes that spyware companies have used to avoid most accountability requirements. In fact, the practice of having subsidiaries under different names in countries that require little to no oversight, so-called regulatory havens (Farrow, 2022) – such as Hungary, Malta, Bulgaria, Singapore and Cyprus (Feldstein et al., 2023) – has become standard. And for every company branch blacklisted, less scrupulous successors are destined to emerge to fill the gap, perpetuating an accountability problem that endangers fundamental rights (Silberman, 2024).

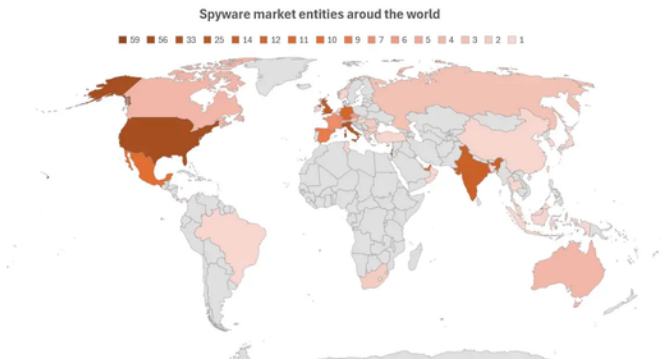


Figure 2. Spyware market entities (subsidiaries included) around the world. Data source: THE STATE OF SPYWARE / A COGNITION INTELLIGENCE ANALYSIS (2026). Available at: https://state-of-spyware..com/. Elaboration by the author.

The main representatives of the sector, the governments of the EU, Israel and the United States, should enhance their cooperation to prevent the intrusion of digital systems from being sold to well-known human rights offenders and implement mandatory transparency controls (Feldstein et al., 2023). In particular, given that

Israel is the main spyware manufacturer and exporter globally, its Ministry of Defence should be more attentive towards both the domestic enforcement of its national security and the democratic track records of recipient governments. But, as stated by cybersecurity expert Eva Galperin to The New Yorker: "They keep expecting that the Israeli government will crack down on NSO for this [controversy], whereas, in fact, they're doing the Israeli government's bidding." (Farrow, 2022).

The European Union, despite its relatively rigorous rules on spyware outflow and trade already in force, remains a favourable environment for the development of these kinds of technologies (Feldstein et al., 2023). Nonetheless, not even its members are safe from them. On July 3, 2026, the Citizen Lab stated that Stelios Kouloglou, a member of the PEGA Committee, reported having his devices infected with Pegasus while actively researching said malware and its implications (Scott-Railton et al., 2026). Five days later, on July 8, 2026, the European Parliament held an emergency session following the formal request by the LEFT and the Greens/EFA groups (Athens Times Newsroom, 2026). In a prior declaration, Dunja Mijatović, Commissioner for Human Rights of the Council of Europe until 2024, affirmed how it is "virtually unimaginable that the use of Pegasus or equivalent spyware could ever be considered in accordance with the law and the necessary safeguards as outlined by the European Court of Human Rights." (Mijatović, 2023).

A Foregone Conclusion

The NSO Group case forces a conclusion that most policy analyses tend to resist: accountability, as currently intended and practised, does not constrain commercial spyware. It legitimises it. The industry is now estimated to be worth approximately twelve billion dollars per year (Hiebert, 2023), and every judicial verdict ultimately establishes a price. Every regulatory blacklist ultimately confers the status of a newsworthy geopolitical actor. Every parliamentary committee investigation, including the one whose members were directly surveilled with the very tool under scrutiny, demonstrates that the technology is powerful enough to compromise the institutions designed to govern it. Ultimately, every academic report, including this one, contributes to envisioning Pegasus as an object of study and strategic analysis rather than a dangerous tool to be abolished.

The question, then, is not whether NSO Group will survive its legal battles, its lobbying campaigns, or its contested strategic status. It inevitably will. The question is whether liberal democracies are willing to acknowledge what the evidence already suggests: they have collectively created a market that is intrinsically incompatible with the rule of law, and the framework deployed to govern it serves primarily to manage appearances rather than actual behaviour.

Omri Lavie, NSO co-founder, clearly said that what his company does is "essential both for the State of Israel and for the world", and he may be right.

However, if such technology already has the power to resist any formalised obstacle placed before it, demanding better regulation is not a conclusion; it is a way of avoiding one. It is that we have already decided, through inaction and selective enforcement, that some tools are above the law. The NSO Group did not reach that conclusion. We did.

References

Albanese, F. (2025). From economy of occupation to economy of genocide: Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967 (A/HRC/59/23). United Nations Human Rights Council. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf

Amnesty International. (2021, July 18). Forensic methodology report: How to catch NSO Group's Pegasus. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Athens Times Newsroom. (2026, July 6). Stelios Kouloglou: Emergency debate at European Parliament over surveillance allegations. Athens Times. https://athens-times.com/stelios-kouloglou-emergency-debate-at-european-parliament-over-surveillance-allegations/

Blessing, J. (2024, January 26). A notorious Israeli spyware firm wants to use the Gaza war to make a comeback. The Hill. https://thehill.com/opinion/cybersecurity/4433419-a-notorious-israeli-spyware-firm-wants-to-use-the-gaza-war-to-make-a-comeback/

Cohen, M. S., & Freilich, C. D. (2024). Israel: The making of a global cyber power (Mideast Security and Policy Studies No. 209). Begin-Sadat Center for Strategic Studies, Bar-Ilan University. /api/wp-media/2024/10/MSPS209web.pdf

Davies, H., & Kirchgaessner, S. (2024, July 25). Israel tried to frustrate US lawsuit over Pegasus spyware, leak suggests. The Guardian. https://www.theguardian.com/news/article/2024/jul/25/israel-tried-to-frustrate-us-lawsuit-over-pegasus-spyware-leak-suggests

De Martin, E. (2024). From shadows to spotlight: Analyzing NSO Group's cyber-surveillance legitimation practices in Israel [Master's thesis, Charles University]. Charles University Digital Repository. https://dspace.cuni.cz/bitstream/handle/20.500.11956/197690/120483612.pdf?sequence=1

Dennett, L. (2018, February 21). Closing the loophole on foreign influence. Project On Government Oversight. https://www.pogo.org/analyses/closing-loophole-on-foreign-influence

Farrow, R. (2022, April 18). How democracies spy on their citizens. The New Yorker. https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

Feldstein, S., & Kot, B. (2023, March 14). Why does the global spyware industry continue to thrive? Trends, explanations, and responses. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf

Frenkel, A. (2024, December 24). Omri Lavie: Rare interview on the storms surrounding Pegasus and NSO [Video]. YouTube. https://www.youtube.com/watch?v=yqfoL2ZDI04

Ganon, T. (2022, February 7). No one was immune: Israel Police Pegasus surveillance list revealed. CTech. https://www.calcalistech.com/ctech/articles/0,7340,L-3928830,00.html

Gray, C. H. (2025). AI, sacred violence, and war: The case of Gaza. Palgrave Macmillan. https://library.oapen.org/bitstream/handle/20.500.12657/98583/9783031815010.pdf

Harwell, D., Nakashima, E., & Timberg, C. (2021, November 3). Biden administration blacklists NSO Group over Pegasus spyware. The Washington Post. https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/

Hiebert, K. V. (2023, March 27). The growing global spyware industry must be reined in. Centre for International Governance Innovation. https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/

Ilnai, I. (2025, April 4). How the US led to Israel's offensive cyber collapse. Israel Hayom. https://www.israelhayom.com/2025/04/04/how-the-us-led-to-israels-offensive-cyber-collapse/

Lieber, D. (2025, March 12). Israeli spyware maker NSO gets new owners, leadership and seeks to mend reputation. The Wall Street Journal. https://www.wsj.com/tech/israeli-spyware-maker-nso-gets-new-owners-leadership-and-seeks-to-mend-reputation-166ac50e

Lobbying registration: NSO Group [Lobbying Disclosure Act filing]. (n.d.). U.S. House of Representatives, Lobbying Disclosure Act Database. https://lda.gov/filings/public/filing/9447bf56-aefd-4570-b574-d0d42a81b032/print/

Lubin, A. (2024). Selling surveillance. Ohio State Law Journal, 85(5), 809–893. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=4136&context=facpub

Mijatović, D. (2023, January 27). Highly intrusive spyware threatens the essence of human rights. Council of Europe, Commissioner for Human Rights. https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights

Mitra, D. (2026, June 10). Meta says NSO continued Pegasus operations despite WhatsApp injunction, seeks contempt ruling. The Wire. https://thewire.in/tech/meta-says-nso-continued-pegasus-operations-despite-whatsapp-injunction-seeks-contempt-ruling

Novo, L. (2025). Spyware blasts: Strict liability for abnormally dangerous activities. Atlantic Council. /api/wp-media/2025/09/Spyware-blasts.pdf

Panagiotopoulos, V. (2026, March 4). Will NSO's US lobbying pay off under Trump? Tech Policy Press. https://www.techpolicy.press/will-nsos-us-lobbying-pay-off-under-trump/

Rubin, S. (2022, January 18). Israeli police accused of using Pegasus spyware on domestic opponents of Netanyahu. The Washington Post. https://www.washingtonpost.com/world/2022/01/18/israel-pegasus-activists-spyware/

Scott-Railton, J., Marczak, B., Abdul Razzak, B., Pundyk, K., Anstis, S., & Deibert, R. (2026, July 3). Espionage against the European Parliament: Member of Committee Investigating Spyware hacked with Pegasus (Citizen Lab Report No. 194). University of Toronto, The Citizen Lab. https://citizenlab.ca/research/member-of-committee-investigating-spyware-hacked-with-pegasus/

Silberman, M. (2024). Policing Pegasus: The promise of U.S. litigation for commercial spyware accountability. Georgetown Law Technology Review, 8(1), 245–286. https://georgetownlawtechreview.org/policing-pegasus-the-promise-of-u-s-litigation-for-commercial-spyware-accountability/GLTR-01-2024/

Simons, M. (2024, November 7). Judge weighs sanctions against Israeli spyware company NSO Technologies. Courthouse News Service. https://www.courthousenews.com/judge-weighs-sanctions-against-israeli-spyware-company-nso-technologies/

Trump, D. J. (2016, December 15). President-elect Donald J. Trump nominates David Friedman as U.S. ambassador to Israel [Press release]. The American Presidency Project. https://www.presidency.ucsb.edu/documents/press-release-president-elect-donald-j-trump-nominates-david-friedman-us-ambassador-israel

U.S. Department of Commerce. (2021, November 3). Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities [Press release]. https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

Ward, A. (2023, January 11). Why Israel won't change course on Ukraine. POLITICO. https://www.politico.com/newsletters/national-security-daily/2023/01/11/why-israel-wont-change-course-on-ukraine-00077408

Imprint

Editors: Andrea Guidotti & Sydney Armor
ViSdP: Theodor Himmel
Publisher: EPIS ThinkTank e.V.
Contact: board.external@epis-thinktank.com
ISSN:

Image credits: Cover and p. 9: Alex Shute/Unsplash · p. 19: Protagonist/Unsplash · p. 29: Christian Lue/Unsplash · p. 39: Igor Omilaev/Unsplash · p. 49: Helsinki city centre (credit to confirm) · p. 61: Michał Jakubowski/Unsplash · p. 71: NSO Group logo (credit to confirm) · p. 53, Picture 1: City of Helsinki, photo Sakari Röyskö · Figures: the authors · Author photos: EPIS.

Are you interested in our work?

EPIS is both a network and a think tank in foreign and security policy. The EPIS Network connects students and graduates, supporting their careers. The EPIS Think Tank produces publications in various formats on different regions and topics. Together, they form EPIS—where you can join passively as a network member or actively contribute to publications. Interested? Apply now for an onboarding meeting & follow us on social media!

Find out more on: www.epis-thinktank.com

or visit us on:



The articles and opinions of the authors do not necessarily reflect the views of the EPIS Think Tank e.V. The authors are solely responsible for the academic integrity of their work, including adherence to scholarly standards and proper attribution of sources.

