EPIS Thinktank

Artificial Intelligence & Cybersecurity

Julian ter Hedde

Europe's Struggle for Digital Sovereignty

How US software dominance and legislation is clouding Brussels's independence

3 Main Points

How vulnerable is Europe’s digital infrastructure to foreign control? The ICC case, other European cases and US tech dominance expose the dependence on US software and cloud infrastructures, undermining digital sovereignty. Europe must prioritise cyber independence through investment, cooperation and secure, EU-based infrastructure.

About the Author

Julian is a 21-year-old Dutch aspiring diplomat and Master's student in Diplomacy and Global Goverance at the Brussels School of Governance. He previously studied at the Universities of Leiden and Utrecht, where he build a strong foundation on computational international relations and law. His research focusses on artificial intelligence and improving European legislation, focussing on strenghtening the ethical and democratic foundations.

Europe’s Struggle for Digital Sovereignty

Clouded Independence: Europe’s Struggle for Digital Sovereignty

International law is under digital attack. The United States, long considered Europe’s greatest ally, is increasingly behaving like a cyberbully. Over the past years, several judges of the International Criminal Court (ICC) in The Hague have publicly expressed concern for their personal safety. Some live under permanent protection, with their homes having been bulletproofed (André, 2025; Hadjimatheou, 2025). Yet the most recent threat has not come from physical violence but from the digital world. Earlier this year, Washington allegedly compelled Microsoft to remove the Outlook account that belongs to the ICC chief prosecutor (Agius Saliba, 2025; Hartholt, 2025). This was after the court opened investigations into Israeli officials. Although Microsoft denies doing this, digital forensics suggest otherwise (Clark, 2025). How vulnerable is Europe’s digital infrastructure to political coercion, and what can be done about it?

The ICC incident demonstrates how Europe’s digital systems are exposed to foreign influence. The court, which is located in the Netherlands, relies on American software for its daily communications. When Microsoft, acting under political pressure, restricted access to these tools, it effectively obstructed an international institution from exercising the law. This highlights a new form of geopolitics: cyber-sovereignty through corporate dependency. American tech giants, nominally private actors, can serve as instruments of statecraft. By leveraging their dominance in software and digital infrastructure, Washington can indirectly shape or silence European institutions. This issue transcends diplomacy; it weakens the foundations of international law and European independence. If a global tech company can deny access to judicial data under pressure of a foreign government, sovereignty becomes conditional, defined by corporate loyalty.

The Netherlands alone is already extremely reliant on American cloud services. Law, government, hospitals, physical infrastructure: practically everything could be shut down if the US president orders this (Algemene Rekenkamer, 2025; Consultancy.nl, 2025; ter Rele, 2025; Werken bij de Rechtspraak, 2025). Autonomy and security are sacrificed in the name of efficiency and convenience.

The Netherlands and the ICC are not the only actors affected. Across Europe, comparable instances reveal the scale of the problem. In Germany, the federal government, despite security warnings from its own data protection agencies, and delayed moving away from Microsoft 365 (DATUREX GmbH, 2024; Niebuhr, 2023). France, which once was a proponent of the “cloud de confiance” label (part of which means the cloud has to be owned by a European entity), had its initiative absorbed by American cloud providers who operated with French subsidiary companies (Maisto, Higgins & Dai, 2025). Even the European Commission was criticized for hosting sensitive data on US servers, after which members of parliament asked to relocate to European-controlled infrastructure (Donnelly, 2025). These instances stress that digital dependency is systemic.

It becomes clear just how critical this dependency can be when considering the case of Crowdstrike (Frölke, 2024). In mid-2024, not for the first time, a faulty Microsoft update paralyzed worldwide digital infrastructure. Banks, hospitals, airports, and a wide range of companies experienced simultaneous digital shutdowns (a total of 8.5 million devices). Surgeries were postponed, flights delayed, and companies could not complete their daily tasks. This disruption lasted for only hours and affected less than 1% of all Windows devices, but the impact was clear. The incident revealed that a single corporate error could affect the entire globe. When crucial infrastructure all depends on one foreign provider, operational resilience vanishes.

The core of this issue lies in the imbalance of power, particularly digital power. The United States hosts the largest cloud infrastructures in the world: Amazon Web Services, Google Cloud, and Microsoft Azure. These platforms manage most of Europe's governmental and institutional data. The word "digital sovereignty," according to Tilburg University (2025), refers to the ability of societies to control their data without undue foreign interference. However, in practice this sovereignty is mostly theoretical. The CLOUD Act, adopted by Congress in 2018, allows US authorities to access data stored abroad by US companies (Eurojust, 2022). Therefore, European institutions using these services risk serious exposure. President Donald Trump has already demonstrated his willingness to use corporate power for political leverage.

Apart from government influence, Microsoft's corporate strategy itself raises concerns. Through acquisitions and contractual bundling, the company is dominating both public and private sectors across Europe. Aside from office software, it provides cloud infrastructure, cybersecurity, and AI analytics for many institutions within the EU (Donnelly, 2025). Furthermore, Microsoft's size allows it to undercut or take over emerging European competitors, halting innovation and reducing technological diversity. This means that Europe is increasingly relying on a single company whose interests are not necessarily aligned with European priorities.

Artificial intelligence deepens these dependencies. At the moment, most resources for AI systems are concentrated in US-based clouds (Leprince-Ringuet, 2023). Europe’s AI ecosystem, while it is expanding, still relies on American infrastructures for training and deployment. This reliance raises both technical and ethical concerns. Firstly, sensitive datasets used in law enforcement or healthcare often reside on foreign servers. Secondly, proprietary AI models function as black boxes. Especially in cybersecurity systems, if the architecture is not transparent, Europeans cannot independently assess whether these systems are compromised. To solve this, Europe must securitise digital sovereignty instead of treating it as a matter of economy. This means recognising cloud systems and data infrastructures as a part of Europe’s critical infrastructure in the same way as defence supply chains and energy grids are. If this infrastructure is interrupted, surveilled or repurposed by foreign governments, Europe’s political autonomy is directly at risk (Csernatoni, 2025). Securitising digital sovereignty would require cloud dependency to be integrated into threat assessments.

The European Commission has already initiated efforts such as the Gaia-X project (Gaia-X, 2023), which aims to build a federated, secure data infrastructure for Europe. The European Defence Industrial Strategy (EDIS, 2023) highlights the need to reduce external dependencies in defence supply chains, although it does not specifically target data infrastructure. Meanwhile, the EU's AI Action Plan (2025) aims to improve European technological capacity by building up to five AI gigafactories. Yet, many of these initiatives are still underdeveloped and fragmented.

However, US-EU digital relationships are not completely adversarial. Europe's reliance on American cloud services is partly protected by legal safeguards, dialogue and joint cybersecurity cooperation. Bodies like the EU-US Trade and Technology Council (TTC) aim to mitigate these risks. Furthermore, US tech providers must operate under stringent EU procurement rules and sectoral requirements. Nevertheless, these safeguards only mitigate the problem partly, as they do not eliminate dependency.

It is up to member states to agree on a digital sovereign strategy. The EU's cybersecurity acts, such as the Cyber Resilience Act (European Commission, 2025), do not yet go deep enough in their implementation. Prioritizing European infrastructures as alternatives to American software monopolies would be a step in the right direction. However, regulation alone is not enough to achieve digital sovereignty. It requires stable investments, industrial cooperation, and political will to reduce dependency.

To conclude, the incidents involving Microsoft, from the ICC shutdown to the worldwide system failures, are not isolated problems. They are symptoms of a deeper structural problem: Europe has surrendered control over its digital foundations. In an era where cyber power affects geopolitical influence, this is untenable. Defending the integrity of international law and European governance requires digital independence to become a security priority. European institutions must operate on European infrastructure, protected by European law and developed by European innovation.

Although this path to digital sovereignty is not easily reachable, the alternative—a path of dependence, coercion, and vulnerability—is already here. Europe is faced with a choice: to continue with borrowed tools of convenience but disruption, or to reclaim control of a free, secure, and autonomous digital future.

References

Algemene Rekenkamer. (2025, January 15). Het rijk in de cloud. https://www.rekenkamer.nl/publicaties/rapporten/2025/01/15/het-rijk-in-de-cloud

Agius Saliba, A. (2025, June 5). The effect of the sanctions imposed by the United States on the functioning of the ICC (Parliamentary question P-002270/2025). European Parliament.

André, A. (2025, July 1). Palestina-onderzoeker van het Internationaal Strafhof stapte op na bedreigingen. Trouw.

Clark, S. (2025, June 2025). Microsoft didn’t cut services to International Criminal Court, its president says. Politico.

Consultancy.nl. (2025, April 24). NS gunt grote AWS-cloudopdracht aan Levi9.

Csernatoni, R. (2025, May 20). The EU’s AI power play: Between deregulation and innovation. Carnegie Europe.

DATUREX GmbH. (2024, November 4). Microsoft Cloud: Authorities dependent despite data protection risks. Externer Datenschutzbeauftragter Dresden.

Donnelly, C. (2025, 24 July). Europe ‘sleepwalking’ into deeper dependency on Microsoft cloud technologies, claims OCC. Computer Weekly.

Eurojust. (2022, December 22). The CLOUD Act.

European Commission. (2021, June 15). EU-US Trade and Technology Council.

European Commission. (2023). The European Defence Industrial Stategy.

European Commission. (2024). Cyber Resilience Act. Shaping Europe’s digital future.

European Commission. (2025, March 6). Cyber resilience act.

European Commission. (2025, April 9). The AI Contingent Action Plan.

Frölke, S. (2024, July 19). Windows-storingsblog 19 juli. NRC Handelsblad.

Gaia-X Association for Data and Cloud. (2023). Website. Retrieved from [Home - Gaia-X: A Federated Secure Data Infrastructure]

Hadjimatheou, C. (2025, June 29). Threat of US sanctions over Gaza forced me out, says ICC lawyer. The Observer.

Hale, C. (2025, June 16). “We’re done” – major government organization slams Microsoft Teams as it drops Windows for good. Techradar.com

Hartholt, S. (2025, May 19). Wake-up call: Microsoft sluit e-mail ICC zonder pardon af. Binnenlands Bestuur.

Maisto, D., Higgins, S. & Dai, C. (2025, June 30). What international customers should know about Microsoft’s sovereign cloud offerings. Forrester.

Niebuhr, M. (2023, January 24). German Data Protection Authorities’ new findings on Microsoft 365 – well founded criticism or missed opportunity? BDO Legal Rechtsanwaltsgesellschaft mbH.

Nilsson-Julien, E. (2025, May 15). Trump’s sanctions on ICC halt tribunal's work, staffers claim. Eurojust.

Leprince-Ringuet, D. (2023, October 17). AI startups need more data centres. France wants to build them. Sifted.

ter Rele, A. (2025, February 22). Amerikaanse bedrijven beheren bijna alle data van onze burgers en overheid – en dat wordt steeds gevaarlijker. Trouw.

Tilburg University. (2025). Digital sovereignty.

Nilsson-Julien, E. (2025, May 15). Trump’s sanctions on ICC halt tribunal's work, staffers claim. Eurojust.

Leprince-Ringuet, D. (2023, October 17). AI startups need more data centres. France wants to build them. Sifted.

ter Rele, A. (2025, February 22). Amerikaanse bedrijven beheren bijna alle data van onze burgers en overheid – en dat wordt steeds gevaarlijker. Trouw.

Tilburg University. (2025). Digital sovereignty.