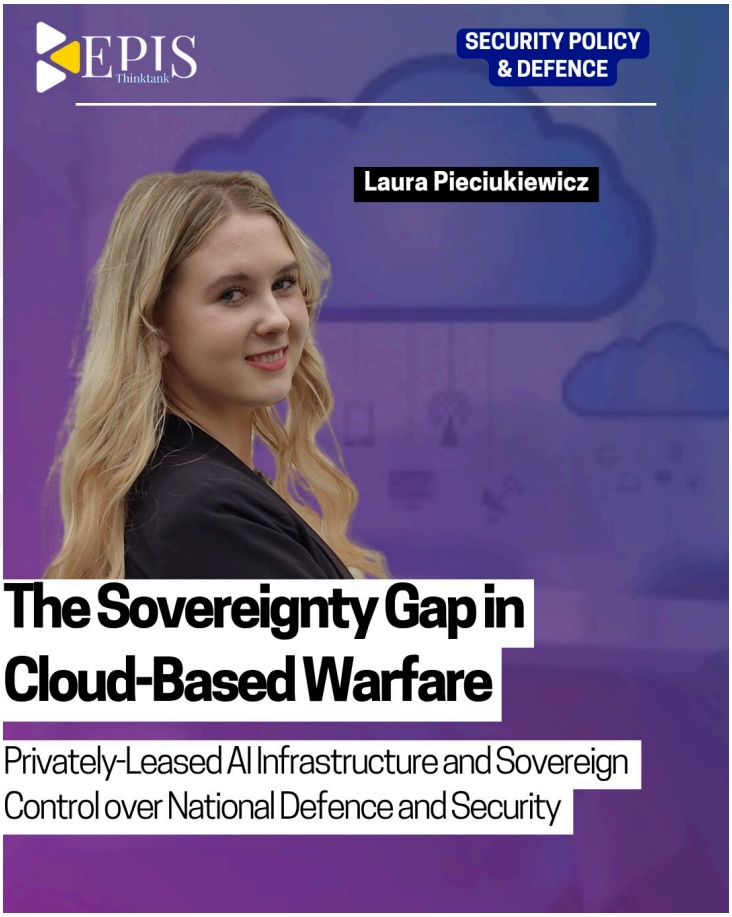
The Sovereignty Gap in Cloud-Based Warfare

1 APRIL 2026

Laura Pieciukiewicz



The Sovereignty Gap in Cloud-Based Warfare: Private-Leased AI Infrastructure and Sovereign Control over National Defence and Security

Introduction

In recent decades, the world has witnessed the rapid expansion and integration of digital infrastructure into the everyday lives of millions of citizens. This ongoing transformation has been particularly noticeable in the military sector, where communication and decision-making have become increasingly dependent on privately-leased AI platforms. As a result, the distinction between state authorities and private corporations is becoming

progressively blurred (Guarascio et al., 2025). Recent cases, such as the involvement of the SpaceX company in the Ukraine war, challenge the traditional concept of state sovereignty and generate questions about the transparency and accountability of corporate actors due to a shortage of legal frameworks governing their actions in the military field (Schaake, 2024). Moreover, the ongoing dispute between the American company Anthropic and the U.S. government demonstrates another relevant aspect of this issue: while governments seek unlimited access to AI infrastructure, their actions are restricted by private companies that condition their use (Gorski & Toomey, 2026). As a result, the emerging AI-driven reality raises a fundamental question: Does the increasing reliance on privately-leased AI infrastructure constitute a transfer of sovereignty in national defence and security from governments to tech corporations?

This paper argues that while there has been no full transfer of sovereignty to tech corporations, the growing reliance on private AI platforms is redefining the way sovereignty is exercised, forming a relationship of substantial interdependence between state authorities and private companies. The topic is particularly relevant in the contemporary world, where military decisions are increasingly subject to cloud-based structures developed by private companies (Schaake, 2024). Thus, by discussing the state-corporate relationship in the military sector nowadays and demonstrating the growing significance of AI infrastructure in national defence, the paper contributes to the existing scholarship on warfare, security and international relations.

To address the research question, this brief will be divided into four main sections, each touching upon a relevant aspect of contemporary warfare. First, the concept of sovereignty will be introduced and situated within the broader context of Big Tech's role in national security and defence. The second section will examine the war in Ukraine, where the privately-owned AI infrastructure significantly shaped the conduct of the conflict, constituting the first prominent example of the impact that such systems exert on military operations. The last section aims to assess the extent to which sovereign control has been transferred to tech corporations and to analyse the entanglement between state authorities and privately-leased AI systems.

Sovereignty in the Age of AI

The recent development and integration of AI platforms into national defence systems has been redefining the long-established relationship between the state and the private sector. This ongoing transformation raises questions about the inevitable implications for state sovereignty, broadly understood as the state's ability to govern and act independently (Bienvenue et al., 2025). Historically, control over political decisions and military capabilities has been considered the core component of this authority. The interests and priorities of private companies and government institutions often diverged, and it was the states that possessed the primary control over warfare infrastructure (Bienvenue et al., 2025).

However, the emergence and rapid advancement of new high technologies undermined the traditional concept of sovereignty (Caceres, 2025). Conventional models of warfare, in which states retain full control over the battlefield, are being reconfigured by increasing reliance on online commercial software (Bienvenue et al., 2025). Governments become more and more dependent on digital infrastructure for coordinating military operations, facilitating communication between different units and storing sensitive administrative data, thus transferring a substantial amount of national information to private entities (Caceres, 2025). It can be argued that sovereignty is no longer equivalent to independence and should rather be perceived in terms of the capacity to act strategically within an interdependent system (Tony Blair Institute for Global Change, n.d.).

This shift is reshaping the operational foundations of national security and defence structures. As military operations increasingly depend on commercial systems and privately-owned platforms, the notion of infrastructural entanglement has gained considerable attention (Javadi, 2025). This concept has emerged as central to debates about contemporary warfare and can be briefly defined as an ongoing process in which state-owned infrastructure becomes directly linked to corporate actors, establishing a relationship of substantial interdependence (Javadi, 2025). This, in turn, generates questions and concerns about the extent to which national authorities nowadays are able to maintain effective control over a state's critical sector. Consequently, defining sovereignty in the age of AI within the context of security and defence seems to be more complex than ever and constitutes a considerable challenge for both governments and states' security.

Case Study: Ukraine as the First Real-World Example

Russia's invasion of Ukraine in 2022 constitutes a prominent example of how significantly digital systems shape contemporary warfare and influence the conduct of the war. While the conflict incorporates the use of conventional military elements, it also heavily relies on digital infrastructure and Big Tech's involvement. Following the destruction of a significant amount of Ukraine's telecom infrastructure by the Russian forces, SpaceX, primarily owned by Elon Musk, became substantially engaged in the conflict by providing satellite internet terminals for Ukrainians (Schaake, 2024). Not only did they enable civilians to maintain internet access, but they also constituted a fundamental operational infrastructure upon which the Ukrainian government and military forces became increasingly reliant. In particular, these satellite internet networks enabled real-time communication between units and facilitated the coordination of drones and artillery operations (Schaake, 2024). However, SpaceX is not the only company that became directly involved in the Ukraine war from its very early stages. Companies such as Microsoft or Amazon Web Services (AWS) have been supporting the management of Ukrainian IT infrastructure, including banking systems and public administration, as well as combating malware

targeting government institutions (Schaake, 2024; Guarascio et al., 2025). In addition, from the very beginning of the conflict, the Ukrainian authorities have been actively cooperating with Palantir, a U.S. IT company. Its software and data are used not only for battlefield intelligence, such as analysing satellite imagery and obtaining drone footage, but also for broader governance functions like documenting war crimes and combating corruption (Bergengruen, 2024). The war in Ukraine exposed vulnerabilities arising from blurred boundaries of sovereignty (Bienvenue et al., 2025). This became especially visible when Elon Musk announced that the services provided to Ukraine are becoming too expensive and might be discontinued unless the U.S. government covers the majority of incurred costs (Schaake, 2024). Taking into consideration Ukrainian dependence on SpaceX's infrastructure and its critical role in the country's resistance, the U.S. authorities were compelled to approve this arrangement (Schaake, 2024). The importance of the service became even more apparent following the recent decision of the company to disable all Starlink terminals used by Russian forces, immediately halting their operations and causing catastrophic disruptions (Hambling, 2026). This raises questions about the balance of power between governments and the private sector, and the risks associated with such strategic interdependence. Indeed, states' autonomy in decision-making and capability to operate independently relies on the alignment of government interests with those of corporate actors (Javadi, 2025). This constitutes a challenge, especially given the importance of corporate decisions and their influence on military operations. Thus, the Ukrainian case demonstrates how contemporary warfare is no longer determined solely by military capabilities, but rather by a multi-layered combination of state authority, AI-driven infrastructure and the power of corporate actors.

Analysis – Transfer or Transformation?

The evidence presented in the abovementioned section suggests that although the increasing reliance on private tech corporations is undeniable and can be analysed based on real-world examples, it does not constitute a complete transfer of sovereignty to the private sector. High technology is influencing decisions, but it has not fully replaced the traditional models of warfare; instead, it has redefined the ways in which it is coordinated and conducted (Bienvenue et al., 2025). As analysed in the section above, the example of Ukraine demonstrates the intertwinement of traditional and modern forms of military engagement, combining conventional weaponry with advanced AI infrastructure. Under these circumstances, the scenario that becomes more and more plausible is the one in which tech giants merge with state institutions into a hybrid system of governance and political management (Volodenkov & Fedorchenko, 2022). Thus, this development does not indicate a transfer of sovereignty but rather suggests a structural shift, where state authority in national security is increasingly exercised with the help of privately-owned digital infrastructure. A timely example relevant to this dynamic trend is the ongoing clash between Anthropic, a leading

American AI company, and the U.S. government. The dispute concerns the use of the company's technological infrastructure, particularly Anthropic's proposed safeguards, which the Pentagon deemed unacceptable, including the reluctance to allow the deployment of its AI platforms for mass domestic surveillance and autonomous weaponry (Frenkel, 2026). Following this declaration, the Trump administration ordered all entities in the U.S. defence sector to cease any commercial engagement with the company, while simultaneously labelling it a supply chain risk (Gorski & Toomey, 2026). Under such circumstances, the AI sovereignty paradox emerges: states aim to preserve sovereign control over critical technologies, while simultaneously being constrained by powerful corporate actors that develop them (Froman, 2026). Thus, the case of Anthropic depicts the tensions that arise between state authorities and private firms in light of growing interdependencies. Nevertheless, in debates on AI and privately-owned digital infrastructure, it is necessary to consider the underlying motivations of corporate actors. Most of the time, their interests are neither neutral nor patriotic, but rather commercial and driven by market valuations or capital investments (Bienvenue et al., 2025). Issues like ethical restraint or public transparency often remain secondary, and tech companies engage in decision-making that aligns with their own commercial strategies (Bienvenue et al., 2025). These circumstances raise important questions not only about accountability, but also about digital rights and fundamental freedoms. Big Data systems are increasingly trained to perform a wide array of functions, including analysing digital user traces, which become a fundamental instrument to gaining control over society (Volodenkov & Fedorchenko, 2022). On top of that, although tech companies are subject to regulations concerning technical and administrative ways of managing their firms, there exists no provision on how they ought to act in the event of military operations (Schaake, 2024). Thus, the access to citizens' private information coupled with a shortage of relevant provisions in international law may lead to a dangerous concentration of power in the private sector. And although tech companies adhered to international norms in Ukraine's case, there is no guarantee that they will abide by human rights principles and ethical standards in the future, especially given their commercial interests (Schaake, 2024). Referring to the Anthropic case, the U.S. government believes that it should be allowed to use artificial intelligence for any lawful reason, which, in the context of regulatory gaps, constitutes a significant threat to citizens' privacy and safety of their personal data (Gorski & Toomey, 2026). Moreover, countries are likely to adopt varying approaches to AI oversight, which poses the question of who, and under what conditions, controls the rapidly evolving technologies. Thus, this regulatory uncertainty highlights the difficulties of incorporating AI systems into national defence structures, while preserving the decision-making autonomy and safeguarding citizens' interests.

Conclusion

To conclude, this brief examined the multi-dimensional concept of state sovereignty within the context of national security and defence. By looking at the relationship between the state authorities and powerful corporate actors, it became evident that the increasing reliance on privately-owned AI platforms reformulates the way sovereignty is exercised. In Ukraine, the government's capacity to coordinate military operations was heavily dependent on private infrastructure, which became critical to Ukraine's resistance. On the other hand, the Anthropic case demonstrates the ultimate power that the U.S. government retains over tech companies and the complex relationship that is formed between those actors. Thus, it can be concluded that sovereignty in national security is less about complete independence but rather the ability to adapt and be able to safeguard one's interests in an advancing world.

References

Bergengruen, V. (2024, February 8). *How tech giants turned Ukraine into an AI war lab*. TIME. https://time.com/6691662/ai-ukraine-war-palantir/

Bienvenue, E., Kelton, M., Rogers, Z., Sullivan, M., & Ford, M. (2025, December 1). *Private tech companies, the state, and the new character of war*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies?lang=en

Caceres, D. G. (2025). Digital Sovereignty in the Cloud and International Law: Towards a Balance between State Autonomy and Transnational Cyber Governance. *Latin American Journal of European Studies*, *5*(2), 84-105.

Frenkel, S. (2026, March 17). *Anthropic and the Pentagon clash over national security risks*. The New York Times.

Froman, M. (2026, February 27). *The AI sovereignty paradox at home and abroad*. Council on Foreign Relations. https://www.cfr.org/articles/the-ai-sovereignty-paradox-at-home-and-abroad

Gorski, A., & Toomey, P. (2026, March 9). *Congress must prevent AI surveillance. The Anthropic feud proves it*. The Guardian.

Guarascio, D., Coveri, A., & Cozza, C. (2025). Big tech and the US digital-military-industrial complex. *Intereconomics, 60*(2), 81–87. https://doi.org/10.2478/ie-2025-0017

Hambling, D. (2026, February 6). *Starlink shutdown: Musk throws Russian forces into chaos*. *Forbes*.

Javadi, M. (2025). Infrastructural entanglement and cloud hyperscalers in contemporary warfare: Insights from Ukraine, Israel and Taiwan. *Contemporary Security Policy*, 1-38. https://doi.org/10.1080/13523260.2025.2593247

Schaake, M. (2024, September 26). *Tech companies aren't just going to war. They're owning the battlefield.* Fast Company.

Tony Blair Institute for Global Change. (n.d.). *Sovereignty in the age of AI: Strategic choices, structural dependencies*.

Volodenkov, S., & Fedorchenko, S. (2022). Digital human rights: risks, challenges, and threats of global socio-political transformations. *Cuestiones Constitucionales*, 279-316. https://doi.org/10.22201/iij.24484881e.2022.46.17057