Date: May 14, 2025

Source: https://aipolicylab.se/aipex/

Civil Sector Vulnerabilities and NATO's Strategic Role: The Case for International AI Governance

Jason Tucker

Researcher, Institute for Futures Studies, Sweden and Adjunct Associate Professor, AI Policy Lab, Department of Computing Science, Umeå University. jason.tucker@iffs.se

Adapted from a presentation given at the NATO Science for Peace and Security Programme, Advanced Research Workshop "Clicking the Pause: The Role of Transatlantic Cooperation in AI Supervision", Salamanca, Spain, 8-9 May 2025.

As AI becomes increasingly embedded in critical societal functions, the need for robust, internationally coordinated governance grows more urgent. While some national and regional regulation of AI is emerging, applications in defence and international security often remain exempt from these initiatives. This historical separation between civil and defence sectors is understandable given the unique operational requirements of the military. However, it risks creating a false dichotomy—suggesting that AI use in civil domains is largely divorced from international security concerns. However, the geopolitical implications of AI in the civil sector are profound and escalating (Schaake, 2024).

To illustrate this, healthcare provides a concrete and urgent example. Across NATO members and partners, localized and largely disconnected decisions are being made to adopt small-scale AI solutions in healthcare. With states having limited capacity to develop in-house solutions, they often turn to external actors. Doing so means that they are then subject to a complex and opaque web of global supply chains and international actors. This poses substantial risks, including vulnerabilities to cyber-attacks, dependencies on potentially hostile states or corporations, and strain on critical infrastructure to support its adoption.

The growing instability of the international order compounds these challenges. The United States has recently exhibited unpredictability in both its Administration and its corporate tech sector. Even if diplomatic relations are maintained, trust at the local level is harder to rebuild. Working with partners whose long-term reliability is in question introduces significant risk, and other non-traditional partners become more appealing. Where these actors are not aligned with NATO, this could be a vulnerability.

Moreover, the adoption of AI in the civil sector has been driven by techno-solutionism— the prioritisation of technological fixes that neglects broader societal and security trade-offs, as well as potentially more appropriate non-technical solutions. It glosses over the reality that AI, as a socio-technical system is embedded in cultural, institutional, and ethical contexts and requires participation from a broad range of actors to function at its best.

Healthcare systems are particularly susceptible to this narrative (Strange and Tucker, 2024). They face resource constraints that limit the capacity to develop, implement, and secure AI technologies. Combined with the dominant discourse being that AI is the only and best way to solve a broad range of healthcare issues, everyday actors in healthcare are facing pressure to adopt AI where they can. At the same time, NATO's security infrastructure is drawing from the same limited resource pool—particularly in terms of skills, energy, data infrastructure, and cybersecurity capacity. Without careful coordination, this could lead to a zero-sum scenario, undermining societal resilience and military advantage.

Cybersecurity threats to healthcare are well documented. The World Health Organization has recognized that cyber-attacks targeting health systems have considerable consequences in terms of public health and international security (WHO, 2024). In 2021, WHO reported that one-third of global healthcare institutions had suffered at least one ransomware attack in the preceding year (Mishra, 2024). The European Union reported that in 2023, healthcare was the most targeted critical sector in cyber-attacks (WHO, 2024). During the COVID-19 pandemic, healthcare was not just a target but a vector for disinformation and destabilisation by state and non-state actors alike.

Given these risks, decisions about AI adoption in critical civil sectors like healthcare cannot be made in isolation from geopolitical and security considerations. Yet most local actors are not equipped to understand or navigate these complex dynamics. The absence of coherent guidance or frameworks linking AI adoption to national and international security exacerbates vulnerability, weakens societal resilience, and increases dependence on untrustworthy partners.

Global AI governance is essential. It can establish the guardrails necessary to manage these risks and guide responsible adoption of AI technologies across sectors. NATO has a critical role to play here. By integrating civil sector AI governance into its strategic thinking, and engaging with the Allies on this, NATO can help ensure that AI adoption enhances—not undermines—resilience and collective security. This will allow for a more realistic assessment of the trade-offs involved in AI adoption, especially in sectors like healthcare

that are both vital to public well-being, are particularly vulnerable to attack and a conduit for hostile actors to cause societal disruption.

NATO's role here should be seen as complementing other international AI governance efforts, such as those by UNESCO, OECD and the EU etc. This would ensure that these governance structures do not become dominated by military priorities and bridge the gap between the defense and civil sector. Democratic safeguards, such as civil society oversight or public reporting, for any NATO-related initiatives affecting the civil sector, would also be essential. As would multidimensional and multidisciplinary views on civil resiliency frameworks.

AI in the civil sector is not a technical or administrative matter alone—it is a strategic issue with implications for the stability, security, and cohesion of NATO members' and partners' societies. Only through coordinated, international governance, can we navigate this new terrain with the prudence and foresight it demands.

References

Mishra, V., (2024) Cyberattacks on healthcare: A global threat that can't be ignored, UN News, https://news.un.org/en/story/2024/11/1156751.

World Health Organization., (2024), Ransomware Attacks on Healthcare Sector 'Pose a Direct and Systemic Risk to Global Public Health and Security', Executive Tells Security Council, https://press.un.org/en/2024/sc15891.doc.htm.

Schaake, M., (2024). The Tech Coup. Princeton University Press.

Strange, M. and Tucker, J., 2024. Global governance and the normalization of artificial intelligence as 'good' for human health. AI & SOCIETY, 39(6), pp.2667-2676.

Further Information This article is part of the Politics of AI & Health: From Snake Oil to Social Good funded by The Wallenberg AI, Autonomous Systems and Software Program – Humanity and Society (WASP-HS).

Keywords (comma separated):

NATO, Civil Sector, Artificial Intelligence, Security, Healthcare, Governance