The Role of Private Actors in Military AI Governance

Elza Ganeeva, Independent Public Affairs Advisor, Netherlands

The Washington DC Conference on the Social Sciences 2026
Official Conference Proceedings

Abstract

The integration of artificial intelligence, AI, into military operations is accelerating, with applications spanning the entire spectrum of warfare, from strategic planning to execution. In this context, the private sector, particularly major AI developers, has assumed a greater role not only as a technology supplier but also as a stakeholder in shaping policies, standards, and broader discourses at both national and international levels. Grounded in security governance theory and literature on the role of private actors, this study examines military AI governance through the lens of Microsoft's cooperation with the Israeli government. It draws on critical discourse and document analysis to explore how legal, principle-based, and corporate frameworks govern the use of Microsoft's technologies in this context. The analysis reveals that while Microsoft has developed a robust internal AI governance architecture and plays an increasingly prominent role in global debates on responsible AI, its norm-setting influence appears limited in high-stakes security contexts. This case suggests that the role of private actors in global governance, often portrayed in modern academic discourse as increasingly growing, is more nuanced in sensitive security environments, where state actors continue to exert dominant influence. The case also points to the limitations of soft law, voluntary commitments, and corporate frameworks in effectively addressing the realities of military AI deployment and highlights the need for clearly defined responsibilities and oversight mechanisms applicable to both states and private actors.

Keywords: security governance, military AI governance, private actors

iafor
The International Academic Forum
www.iafor.org

Introduction

Military adoption of AI is accelerating, with the technology increasingly integrated across the entire cycle of warfare, from operational planning to targeting and post-operation analysis. While AI may improve military efficiency and support compliance with international humanitarian law through enhanced precision and decision-making, its deployment also creates significant risks, including flawed targeting, unlawful attacks, and increasing risks of civilian casualties (International Committee of the Red Cross, 2021).

The current international debate has largely focused on whether existing legal frameworks, particularly international humanitarian law, IHL, adequately regulate military AI. However, far less attention has been devoted to the governance of AI systems developed by private actors for commercial purposes and later deployed in military contexts. This gap is increasingly significant as commercial technologies not originally designed for battlefield decision-making are integrated into armed conflict (Biesecker et al., 2025).

Building on literature suggesting that private actors are gaining authority and legitimacy in global governance (Abrahamsen & Williams, 2007; Bureš & Carrapico, 2017; Cutler, 1999; Finnemore & Sikkink, 1998; Hall & Biersteker, 2002; Khanal et al., 2024), this research examines the role of technology companies in shaping the governance of military AI. It focuses on the Microsoft-Israel partnership as a case study to explore how private-sector actors influence the emerging global governance landscape of military AI.

The case illustrates the complex dynamic between commercial technology development and state military deployment. Microsoft is a prominent private actor actively contributing to global AI governance. At the same time, Israel has emerged as a leading state actor in the military application of AI, particularly in the Gaza conflict following the Hamas attacks of 7 October 2023 (Grim & Ahmed, 2025). Reports indicate that Israel relies extensively on Microsoft's services in support of military operations (Abraham, 2025; Biesecker et al., 2025), raising questions about the role of private actors in both the operational and normative dimensions of military AI governance.

In this context, the research asks: What does the Microsoft-Israel cooperation reveal about current military AI governance mechanisms? Specifically, the study examines whether the increasing prominence of private actors in AI governance discourse translates into meaningful authority over the deployment of military AI, or whether states remain the dominant actors in determining how such technologies are used in practice.

Literature Review

Traditionally, as the governance concept was closely associated with the state, security was long considered an inherently state-bound responsibility tied to sovereignty and the "*state's monopoly on the legitimate use of physical force within its territory*" (Weber, 1947, p. 78). The state was seen as the principal actor responsible for maintaining and providing public order and security. However, since the end of the Cold War, the concept of security has significantly transformed, expanding beyond its conventional military focus to include political, economic, and societal dimensions (Hänggi & Tanner, 2005). In this sense, security is no longer limited to the battlefield but a broader field encompassing new threats. As a result, a new framework of security governance has emerged (Abrahamsen & Williams, 2009), reflecting both the

diversification of threats and the re-configuration of authority manifested in the rise of private actors and new arrangements involved in providing security.

Previously, the expanding authority of private, non-state actors has been synonymous with state failure and eroding sovereignty when states outsource or lose control over security functions (Abrahamsen & Williams, 2007). However, the involvement of private actors does not necessarily mean the retreat or failure of the state but rather signals a transformation in how authority is produced and exercised across networks of public and private actors. While private security may be controversial and occasionally operates at the margins of legality, private actors also engage in a range of lawful activities, often in coordination with public security forces.

One example is a growing class of non-security private actors whose core business is outside traditional security but whose infrastructures, platforms, or services have become essential for security governance. These include tech firms, financial institutions, infrastructure owners and operators, and others. While security is not their main mission, these actors may still intentionally contribute to it, deliberately and purposefully engaging in actions that address security concerns rather than doing so incidentally as a by-product of their operations. In other words, their involvement goes beyond accidental effects and becomes a deliberate effort to deal with (in)security within a given environment (Abrahamsen & Williams, 2007).

This growing involvement of private actors in security governance can also be explained by the post-9/11 "*securitization"* trend in many Western states, where governments began actively enlisting them to help manage national security challenges. This development, in turn, promoted the approach of "*responsibilization*," in which private businesses and other non-state actors are expected to take more responsibility for their own safety and security (Garland, 2001). As a result, the lines between public and private security have become blurred (Wood & Dupont, 2006), with more entities without a background in security becoming involved in the delivery of security functions.

As the engagement of private actors deepens, they also begin to assert and perform functions traditionally reserved for public authority, such as setting agendas, establishing boundaries, and contributing to the provision of global public goods like order and security (Hall & Biersteker, 2002). In other words, private actors operate across both domestic and international spheres in ways that challenge established notions of state sovereignty and public authority (Cutler, 1999).

However, private entities remain unaccountable to citizens. They are neither elected by citizens nor subject to democratic oversight but rather accountable to shareholders and the market itself. In this context, tech companies represent a peculiar set of private actors within global security governance. Unlike traditional public authorities, the power of tech companies does not derive from democratic legitimacy, legal mandate, or intergovernmental delegation. Instead, it is grounded on market dominance, technical expertise, and infrastructural control. While not traditional security providers, their platforms and products are deeply embedded in international security, from cybersecurity to applications in conventional military operations. They exclusively control "*computational infrastructure,"* a globally distributed network comprising data centers, digital platforms, mobile devices, and communication networks that are proprietary, layered, and deeply interdependent (Sharon & Gellert, 2024).

As digitalization accelerates across all sectors, including defense, tech companies have become critical enablers of essential functions, creating structural dependencies when other actors largely rely on their infrastructure and technologies. They also enforce their own "*governance regimes"* through platform-specific policies and terms of use, effectively acting as regulators within their domains (Khanal et al., 2024). As a result, private companies can be seen not merely as partners to the public sector but as "*norm entrepreneurs"* – agents, constructing cognitive frames, calling attention to issues, or even creating them (Finnemore & Sikkink, 1998).

By setting industry standards, entering partnerships with international institutions, advocating for policy changes, co-authoring academic research, and shaping information environment, they are embedding themselves in security governance. Private actors are no longer just advising or supporting state efforts in providing security but also redrawing the boundaries of who governs security and how. The central role of their infrastructure, technologies, and proprietary knowledge, combined with the absence of meaningful counterbalancing alternatives, raises concerns for global governance, particularly in areas with limited public oversight, such as the military domain. As AI becomes increasingly integrated in military planning and operations, tech companies are no longer observers or simply "*objects of regulation"* (Carrapico & Farrand, 2016). They are increasingly architects of the emerging governance rules and norms. But what are these rules?

Microsoft's Approach to AI Governance and Implications for Military AI Governance

This research traces the growing impact of the private sector on AI governance in security, focusing on Microsoft as a revealing case study. While Microsoft's experience cannot be generalized across the tech sector, it offers valuable insights into the expanding role of major tech companies in shaping global governance frameworks, including in the most sensitive areas of technological development. Microsoft's engagement in corporate diplomacy has deep roots, particularly in cybersecurity governance, where the company's influence has already drawn academic attention (Fairbank, 2019; Gorwa & Peez, 2020; Hurel & Lobato, 2018).

Building on this foundation, this paper explores how Microsoft has extended its norm-setting reach into the sphere of AI. The dataset includes corporate policies, governance and compliance frameworks, public statements, and other materials. Given the dual-use nature of AI and Microsoft's focus on broader commercial AI, the delineation between its approach to commercial and military governance is often blurred. Accordingly, the analysis integrates both Microsoft's broader AI policy narratives and its defense-specific engagements. These materials are examined using a qualitative interpretive approach informed by Critical Discourse Analysis, drawing on van Dijk's socio-cognitive model (van Dijk, 1993). The analysis focuses on how Microsoft frames its governance role, constructs legitimacy, and advances its policy positions across different institutional contexts. Particular attention is given to argumentation, rhetorical framing, and appeals to broader societal values, as well as to how these narratives relate to the company's practices.

At the center of Microsoft's vision are its Responsible AI principles – fairness, reliability and safety, privacy and security, transparency, accountability, and inclusiveness (Microsoft, n.d.-a), which underpin a range of corporate resources and requirements such as the Responsible AI Standard, Transparency Reports, Enterprise AI Services Code of Conduct, or the Sensitive Use Case Framework (Microsoft, 2022, 2023a, 2024a). While they set expectations for development and use of AI, they remain high-level and it is not clear how these principles and

requirements are operationalized in the company's internal decision-making, development, testing, evaluation, and auditing of AI systems designed for sensitive use cases, such as defense and security. Moreover, the company acknowledges that at the later stages, it has limited visibility into how customers deploy the company's technologies, especially on their own infrastructure (Microsoft, 2025). As a result, meaningful oversight during the later stages of use is largely confined to legal and contractual mechanisms, such as terms of use and broader compliance requirements.

In parallel, Microsoft advances its governance approach through policy documents such as the "*AI Blueprint for the Future"* (Microsoft, 2023b), proposing measures like safety standards and regulatory interoperability structures aligned with the company's technical architecture. In the document, Microsoft advocates for expanded public-private partnerships as a means of addressing economic and societal challenges associated with AI. This framing is indicative of a "*technosolutionist"* discourse – the idea that social problems should be addressed through technologies rather than policy reforms, and the progress stems from the private sector, not the state (Morozov, 2013). A similar approach is reflected in its "*Global Governance Book,"* which outlines the company's vision for international AI governance and favors flexible, principle-based, soft law approach – "*a technocratic, adaptive, and flexible framework built on cooperation among smaller groups of like-minded states"* (Microsoft, 2024b, p. 51), over formal international treaty-based models. In effect, Microsoft positions itself as a governance stakeholder, evaluating international governance models and suggesting their configuration and participants.

At the international level, Microsoft institutionalizes its influence via strategic partnerships such as with UNIDIR, launching the Roundtable for AI, Security and Ethics, RAISE, (UNIDIR, 2024) facilitating direct engagement with national policymakers and contributing to the UN discourse on international security (Microsoft, 2021). The company also engages in standard-setting processes (Microsoft, 2024b), academic collaborations (Microsoft, n.d.-b), and multistakeholder initiatives, reinforcing its role in shaping governance discussions and knowledge production.

At the national level, the engagement with the U.S. government and defense sector, positions Microsoft as one of the key stakeholders in shaping policy and norms, aligned with U.S. goals of tech leadership. The U.S. government is both one of Microsoft's most important clients and a strategic partner in defense (Lopez, 2022; Townes-Whitley, 2021). Recognition by influential military power as a competent and trusted actor further enhances Microsoft's legitimacy in the eyes of other governments, institutions, and private actors.

Leveraging this comprehensive governance architecture, the company effectively acts as a norm entrepreneur in the AI governance field, influencing policy agendas, framing the discourse, and building institutional and public trust in both its technologies and the broader societal and economic potential of AI. However, limited visibility is offered in the company's efforts for implementing its responsible AI commitments. It remains unclear how Microsoft's principles and requirements are operationalized in practice and what oversight exists over the end use of its technologies. As AI is increasingly deployed in international conflicts, the lack of transparency from both technology developers and their end-users raises significant concerns. Suggested informal, principle-based frameworks, rooted in soft law and voluntary commitments, often lack clarity, accountability, and enforcement mechanisms.

Israel's Approach to Military AI Governance

Building on the approach applied to Microsoft, this paper uses Critical Discourse Analysis, CDA, to examine how Israel positions itself in international debates on military AI. The analysis draws on Israel's voting behavior and official statements in the United Nations General Assembly on AI in the military domain and lethal autonomous weapons systems, LAWS (Israel, 2024), its engagement with the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (Council of Europe, 2024), and the development of its domestic legal and policy frameworks. It also incorporates operational practice, drawing on statements by Israeli military officials and independent media investigations, which often provide the only available evidence of real-time military AI applications.

The analysis focuses on how Israel articulates and justifies its use of AI, including through legal and strategic argumentation, rhetorical framing, and narrative positioning. In particular, it examines how AI is presented as enhancing accuracy and effectiveness of military operations, how debates are framed through selective legal distinctions, and how Israel positions itself as a responsible actor through engagement with international initiatives.

At the international level, Israel participates in key discussions on military AI governance, arguing that the existing international legal frameworks adequately address challenges posed by AI in military contexts (Israel, 2024). In December 2024, the country voted in favor of UN GA Resolution 79/239 on AI in the military domain (United Nations General Assembly, 2024a). While an important step toward consensus-building, the document outlines a general framework, encouraging states to address the opportunities and challenges of military AI, but does not impose substantive constraints or clarify legal obligations beyond broad, principle-based commitments.

At the same time, Israel abstained from voting on the more specific UNGA resolution 79/62 (United Nations General Assembly, 2024b), which is dedicated to the issue of LAWS. Israel's position on LAWS is especially illustrative of its broader approach. Like other technologically advanced military powers, Israel views these systems as serving both military and humanitarian necessities and upholding compliance with IHL (Israel, 2024, para. 2). In its rhetoric, Israel suggests a flexible approach and maintains that the legality of LAWS should be assessed contextually, depending on specific use cases. Moreover, in Israel's view, even the application of IHL should be based on the operational context and should "*not be equated with blanket declarations about the legality or illegality of a weapon per se"* (Israel, 2024, para. 8).

The country also proposes a distinction between the "*primary rules of IHL*," which it defines as hard, established legal obligations, and "*secondary or supporting concepts"* such as human control, responsibility, foreseeability, or predictability. While it acknowledges the relevance of the "*secondary"* concepts for interpreting and applying IHL, it outlines that they do not constitute legal obligations and should not be treated as binding components of the legal framework (Israel, 2024, para. 9).

In the broader AI governance debate, Israel supports largely declarative international efforts rather than military-specific initiatives suggesting practical constraints or legal commitments. Its participation can be viewed mainly as a reputational strategy aimed at preemptively addressing concerns about its use of AI. For example, in September 2024, Israel joined the Council of Europe's Framework Convention on Artificial Intelligence, Human Rights,

Democracy, and the Rule of Law (Council of Europe, 2024). While the Convention seeks to ensure that AI systems align with human rights and democratic values, it explicitly excludes military applications and activities related to national security (Babická & Giacomin, 2024). As a result, military AI systems developed and deployed by states and private actors fall outside its scope.

At the national level, Israel has not adopted specific legislation regulating AI. The only relevant policy document, the National AI policy (Ministry of Innovation, Science and Technology et al., 2023), sets out non-binding guiding principles, which, as stated in the document, are not legally binding on regulators or organizations. In this context, Israel's operational practices appear to diverge from its declarative commitments, which remain largely non-binding and limited in scope.

The Israeli Defense Forces, IDF, have actively integrated AI into battlefield operations. The IDF describes the adoption of AI as a means of enhancing the "*accuracy and effectiveness*" of its strikes by better managing vast amounts of data and improving intelligence processes while reducing risks of civilian casualties (Bohbot, 2022). Israel has previously used conflicts in Gaza and Lebanon to test and refine AI-powered military solutions. During an 11-day campaign against Hamas in May 2021, the IDF characterized the operations as its "*First AI War."* At that time, Israeli intelligence officials described AI as a "*force-multiplier*," enabling significantly higher volumes of airstrikes than in previous conflicts (Biesecker et al., 2025). This activity has reached a higher level in the military operations on Gaza, with the IDF, reportedly integrating AI across multiple dimensions of warfare, including surveillance, target identification, operational planning, and execution.

The IDF emphasizes that AI-enabled systems help identify targets, while final decisions are made by operational commanders, who assess the compliance with international law by weighing the military advantage against the potential collateral damage. According to Israeli officials, when AI is involved, several layers of human oversight are always in place. However, available reports point to a significant increase in the scale and speed of strike approvals. As one Israeli commander reportedly noted, while previously a single airstrike required a team of up to 20 people a day, AI-assisted targeting now enables the approval of hundreds of attacks per week (Biesecker et al., 2025), which raises questions about the compliance with IHL principles.

Beyond general statements that the use of such technology complies with international law Israel discloses little specific information about the operational details or governance structures of its military AI systems. However, available reporting suggests that the use of AI has expanded the scope of targeted individuals and infrastructure, with reported civilian harm and concerns about the extent of human involvement in life-and-death decision-making (Thornhill, 2025).

Governing Military AI: Insights From the Microsoft-Israel Collaboration

Amid the deepening cooperation between Israel and the U.S. tech corporations, the Microsoft-Israel partnership stands out particularly. These relationships have been developing for years and significantly intensified after the Hamas attack on 7 October 2023. Microsoft is one of the biggest cloud and AI service providers for the Israeli military. In 2021, the IDF signed a three-year contract with Microsoft valued at USD 133 million, reportedly making Israel one of

Microsoft's largest government customers following the U.S., and one of its top 500 clients globally (Biesecker et al., 2025).

These relationships are mainly managed through the Israeli Ministry of Defense, MoD, overseeing Microsoft's services integration across all major Israeli military infrastructures with hundreds of active subscriptions for specific divisions, units, bases, and projects (Grim & Ahmed, 2025). On Microsoft's side, reporting indicates that a team of dedicated employees is responsible for supporting the Israeli MoD, including personnel with prior experience in Israeli military intelligence. Support for IDF personnel includes both technical assistance and skills-development activities, such as meetings and professional workshops. Between October 2023 and June 2024 alone, the Israeli MoD reportedly received 19,000 hours of engineering support from Microsoft at a cost of USD 10 million (Abraham, 2025).

According to reports, Microsoft provides its cloud platform, Azure, and other services, including AI, to support the growing technological needs of the Israeli military. In 2024, the demand for such services increased to 200 times the level prior to the October 7 attack (Biesecker et al., 2025). The expanded use of services is registered across various units of the IDF, including air, ground, and naval forces, as well as intelligence (Frenkel & Odenheimer, 2025). In particular, the volume of data stored in Microsoft's local data centers reportedly doubled and the IDF's use of Microsoft servers increased by nearly two-thirds within the first two months following the October 7 attack (Abraham, 2025).

Reports describe Microsoft cloud services being used to compile, transcribe, translate, and analyze large-scale data, including phone calls, text messages, and social media, which are then cross-referenced with internal targeting systems to assist in locating individuals (Biesecker et al., 2025). One example is the *Rolling Stone* system, used by the Israeli army to manage the population registry and movement of Palestinians in the West Bank and Gaza, which is associated with Microsoft cloud infrastructure (Abraham, 2025).

In parallel, advanced AI models are allegedly provided through OpenAI, the developer of ChatGPT, in which Microsoft is the largest investor (Novet, 2023). Since 2021, Microsoft has offered ChatGPT services through its cloud platform (Shaw, 2021). Revealed Microsoft documents have shown that the Israeli military purchases OpenAI tools as part of a "bundled package" provided by Microsoft (Grim & Ahmed, 2025). In 2023, the IDF reportedly began using GPT-4, OpenAI's most advanced language model, through Azure. Since October 2023, its use by the Israeli military increased by 20 times compared to pre-war levels (Abraham, 2025).

The IDF has also made extensive use of translation tools. While the specific models used remain unclear, OpenAI has previously acknowledged that its AI-powered translation model, Whisper, can transcribe and translate speech into multiple languages, including Arabic, but may produce inaccurate outputs, including the insertion of content which is not present in the original speech (Burke & Schellmann, 2024). Available reporting further describes instances in which intelligence personnel were affected by inaccurate machine translations from Arabic to Hebrew while identifying targets. It also highlights concerns about operational pressure to rapidly identify threats, when officers are disproportionately relying on AI-generated outputs, resulting in the misidentification of targets.

In May 2025, Microsoft issued a public statement (Microsoft, 2025), confirming its provision of cloud and AI services to the Israeli MoD. In the statement, the company stated that it does

not have visibility into how customers use its software on their own servers or devices. Microsoft also noted that the Israeli MoD is subject to the company's terms of service, including the AI Code of Conduct, which prohibits the use of its services to inflict harm. Following both internal evaluation and external independent review by a third party, the details of which were not disclosed, Microsoft stated that it had found no evidence of the MoD violating the AI Code of Conduct or terms of use. However, the company admitted that it may grant exceptions to these terms and confirmed that such an exception had been granted to the Israeli government in the weeks following the 7 October attack. At the same time, neither the MoD nor the company has disclosed any oversight mechanisms that govern their cooperation in such sensitive contexts, raising questions about whether meaningful governance mechanisms are in place.

Conclusion

The analysis reveals a divergence between formal governance frameworks and operational practice in the use of military AI. Israel's approach to military AI is characterized by its engagement with non-binding international initiatives and the absence of formal national regulation, while its expanding use of AI raises questions about compliance with IHL and related principles in practice. By contrast, Microsoft has developed an extensive AI governance architecture, but limited public information is available on how these principles are implemented in practice. This divergence highlights a gap between state and corporate governance commitments and the real-time application of AI technologies in conflict settings, where transparency regarding safeguards remains scarce, particularly in the absence of oversight mechanisms specific to military AI at both international and domestic levels.

This points to a broader tension in state-private actor partnership in national security, reflecting uncertainty regarding the extent to which private actors like Microsoft can meaningfully influence or constrain the end use of their technologies when engaging with powerful state clients. In this case, Microsoft's influence over the conditions of deployment appears limited. In fact, the dynamic may be reversed, with Israel setting the terms of use in practice and operating beyond the reach of corporate governance frameworks. This finding also adds nuance to the emerging academic consensus that private tech companies are increasingly gaining influence in shaping global governance. Instead, it suggests that in high-stakes security contexts, state actors continue to exert dominant authority, while private-sector influence remains contingent.

This case study also underscores the limitations of soft law and voluntary governance mechanisms in high-stakes domains such as military AI. While states may endorse principle-based commitments, these do not necessarily translate into operational constraints. Israel's engagement with non-binding initiatives has not been accompanied by the development of binding rules or observable limitations in practice. Participation in international debates and the endorsement of declarative documents on military AI governance may therefore function primarily as expressions of alignment rather than mechanisms of accountability.

Finally, ambiguity, lack of transparency, and insufficient public oversight in current state-private actor security relationships constitute a key challenge for emerging military AI governance. While it is difficult to clearly delineate roles and responsibilities in such partnerships, this uncertainty enables an environment where accountability is diffused and control mechanisms, where they exist, do not provide a meaningful constraint. As military AI continues to advance and its deployment in conflict settings accelerates, addressing these gaps

in state-private sector security arrangements will be central to the development of effective governance frameworks aligned with operational realities.

Disclosure

The author worked for Microsoft until 2021. The author's former affiliation with Microsoft did not influence the design, analysis, or conclusions of the research. The work is based solely on publicly accessible information.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

The author used Grammarly, an AI-assisted writing tool for grammar and punctuation correction and minor language refinement. No AI tools were used to generate content.

References

Abraham, Y. (2025, January 23). *Leaked documents expose deep ties between Israeli army and Microsoft*. +972 Magazine. https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/

Abrahamsen, R., & Williams, M. C. (2007). Securing the city: Private security companies and non-state authority in global governance. *International Relations, 21*(2), 237–253. https://doi.org/10.1177/0047117807077006

Abrahamsen, R., & Williams, M. C. (2009). Security beyond the state: Global security assemblages in international politics. *International Political Sociology, 3*(1), 1–17. https://doi.org/10.1111/j.1749-5687.2008.00060.x

Babická, K., & Giacomin, C. (2024, November 5). *Understanding the scope of the Council of Europe framework convention on AI*. Opinio Juris. https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/

Biesecker, M., Mednick, S., & Burke, G. (2025, February 18). *As Israel uses US-made AI models in war, concerns arise about tech's role in who lives and who dies*. AP News. https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108

Bohbot, A. (2022, July 2). *Neshek shover shivyon: Ha-tekhnologya she-takhri'a et ha-ma'arakha ha-ba'a shel Tzahal* [A game-changing weapon: The technology that will decide the IDF's next campaign]. Walla. https://news.walla.co.il/item/3559347

Bureš, O., & Carrapico, H. (Eds.). (2017). *Security privatization: How non-security-related private businesses shape security governance*. Springer. https://doi.org/10.1007/978-3-319-63010-6

Burke, G., & Schellmann, H. (2024, October 26). *Researchers say an AI-powered transcription tool used in hospitals invents things no one ever said*. AP News. https://apnews.com/article/ai-artificial-intelligence-health-business-90020cdf5fa16c79ca2e5b6c4c9bbb14

Carrapico, H., & Farrand, B. (2016). Dialogue, partnership and empowerment for network and information security: The changing role of the private sector from objects of regulation to regulation shapers. *Crime, Law and Social Change, 67*, 245–263. https://doi.org/10.1007/s10611-016-9652-4

Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Cutler, A. C. (1999). The contours and significance of private authority in international affairs. In A. C. Cutler, V. Haufler, & T. Porter (Eds.), *Private authority and international affairs* (pp. 333–379). State University of New York Press.

Fairbank, N. A. (2019). The state of Microsoft? The role of corporations in international norm creation. *Journal of Cyber Policy, 4*(3), 376–394. https://doi.org/10.1080/23738871.2019.1696852

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization, 52*(4), 887–917. https://doi.org/10.1162/002081898550789

Frenkel, S., & Odenheimer, N. (2025, April 25). *Israel uses AI to target Gaza amid rising civilian toll*. The New York Times. https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford University Press.

Gorwa, R., & Peez, A. (2020). Big Tech hits the diplomatic circuit: Norm entrepreneurship, policy advocacy, and Microsoft's cybersecurity tech accord. In D. Broeders & B. van den Berg (Eds.), *Governing cyberspace: Behavior, power, and diplomacy* (pp. 263–283). Rowman & Littlefield.

Grim, R., & Ahmed, W. (2025, January 23). *The Israeli military is one of Microsoft's top AI customers, leaked documents reveal*. Drop Site News. https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud

Hall, R. B., & Biersteker, T. J. (2002). The emergence of private authority in the international system. In R. B. Hall & T. J. Biersteker (Eds.), *The emergence of private authority in global governance* (pp. 3–22). Cambridge University Press. https://doi.org/10.1017/CBO9780511491238.002

Hänggi, H., & Tanner, F. (2005). Promoting security sector governance in the EU's neighbourhood. In N. Lybekk & K. Smith (Eds.), *Challenges for the European security and defence policy* (Chaillot Paper No. 75, pp. 11–26). European Union Institute for Security Studies.

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: Private companies as norm entrepreneurs. *Journal of Cyber Policy, 3*(1), 61–76. https://doi.org/10.1080/23738871.2018.1467942

International Committee of the Red Cross. (2021). *ICRC position on autonomous weapon systems*. https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems

Israel. (2024). *Remarks on the Secretary-General's implementation report* (L.56: "Lethal autonomous weapons systems"). United Nations General Assembly. https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_%282024%29/78-241-Israel-EN.pdf

Khanal, S., Zhang, H., & Taeihagh, A. (2024). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society, 44*(1), 52–69. https://doi.org/10.1093/polsoc/puae012

Lopez, C. T. (2022, December 12). *Department names vendors to provide joint warfighting cloud capability*. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3243483/department-names-vendors-to-provide-joint-warfighting-cloud-capability

Microsoft. (n.d.-a). *Our approach to AI*. https://www.microsoft.com/en-us/ai/principles-and-approach

Microsoft. (n.d.-b). *Artificial intelligence*. Microsoft Research. https://www.microsoft.com/en-us/research/research-area/artificial-intelligence/

Microsoft. (2021, December). *Submission to the OEWG chair's questions on developments in the field of information and telecommunications in the context of international security*. https://documents.unoda.org/wp-content/uploads/2021/12/Microsoft-submission-to-OEWG-Chair-questions-DECEMBER-2021.pdf

Microsoft. (2022, June). *Responsible AI standard, v2: General requirements*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft-Responsible-AI-Standard-General-Requirements.pdf

Microsoft. (2023a). *Put responsible AI frameworks in action*. Microsoft Learn. https://learn.microsoft.com/en-us/training/modules/embrace-responsible-ai-principles-practices/7-put-responsible-ai-frameworks

Microsoft. (2023b). *Governing AI: A blueprint for the future*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Governing-AI-Blueprint-for-the-Future.pdf

Microsoft. (2024a). *AI code of conduct*. https://learn.microsoft.com/en-us/legal/ai-code-of-conduct

Microsoft. (2024b, May). *Global governance: Goals and lessons for AI*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Global-Governance-Book-DIGITAL.pdf

Microsoft. (2025, May 15). *Our statement on technology and the conflict in Israel and Gaza*. https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/

Ministry of Innovation, Science and Technology, Office of Legal Counsel and Legislative Affairs, & Ministry of Justice. (2023). *Israel's policy on artificial intelligence regulation and ethics*. https://www.gov.il/BlobFolder/policy/ai_2023/en/Israels%20AI%20Policy%202023.pdf

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. PublicAffairs.

Novet, J. (2023, April 8). *Microsoft's complex bet on OpenAI brings potential and uncertainty*. CNBC. https://www.cnbc.com/2023/04/08/microsofts-complex-bet-on-openai-brings-potential-and-uncertainty.html

Sharon, T., & Gellert, R. (2024). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. *Information, Communication & Society, 27*(15), 2651–2668. https://doi.org/10.1080/1369118X.2023.2246526

Shaw, F. X. (2021, November 2). *Microsoft cloud at Ignite 2021: Metaverse, AI and hyperconnectivity in a hybrid world*. Microsoft. https://blogs.microsoft.com/blog/2021/11/02/microsoft-cloud-at-ignite-2021-metaverse-ai-and-hyperconnectivity-in-a-hybrid-world/

Thornhill, J. (2025, April 29). *Future weapons – Battlefield AI*. Financial Times. https://www.ft.com/content/802864cb-a680-48ea-837b-32cb31ad09e4

Townes-Whitley, T. (2021, July 6). *Microsoft's commitment to the DoD remains steadfast*. Microsoft Official Blog. https://blogs.microsoft.com/blog/2021/07/06/microsofts-commitment-to-the-dod-remains-steadfast

United Nations General Assembly. (2024a, December 24). *Resolution 79/239*. https://undocs.org/A/RES/79/239

United Nations General Assembly. (2024b, December 2). *Resolution 79/62*. https://undocs.org/A/RES/79/62

The United Nations Institute for Disarmament Research (UNIDIR). (2024). *RAISE: The roundtable for AI, security and ethics*. https://unidir.org/raise/

van Dijk, T. A. (1993). Principles of critical discourse analysis. *Discourse & Society, 4*(2), 249–283. https://doi.org/10.1177/0957926593004002006

Weber, M. (1947). *The theory of social and economic organization* (A. M. Henderson & T. Parsons, Trans.). Free Press.

Wood, J., & Dupont, B. (2006). Democracy, society and the governance of security. *Security Journal, 19*(4), 249–267.

Contact email: elza@raisenl.com