SDU
University of Southern Denmark

Geopolitics of AI Governance

Actors, Norms, and Trends

Collective Policy Brief

Edited by Anna Nadibaidze and Justinas Lingevicius

CENTER FOR WAR STUDIES

March 2026

About the Center for War Studies

The Center for War Studies (CWS), established at the University of Southern Denmark (SDU) in 2012, brings together academics from political science, law, history and cultural studies to contribute to the major debates on the past, present and future of war, as well as its impact on societies. We strive for interdisciplinary research that is relevant to policymakers and the society at large. We aim to contribute to ongoing debates on war and peace by illuminating their multiple dimensions.

We are deeply committed to knowledge exchange with the wider society. We aim to overcome disciplinary barriers and to share our research through engagement with decision-makers from both national and international institutions. Our research also informs our educational programmes at the University of Southern Denmark, notably the Master's programme in International Security and Law (MOISL). Hence, through research excellence and societal relevance, we advance the understanding of the fundamental issue of war and peace. Find out more about the Center and its research at: https://www.sdu.dk/cws.

How to cite this publication and the contributions

Nadibaidze, A., & Lingevicius, J. (Eds). (2026). *Geopolitics of AI Governance: Actors, Norms and Trends*. Odense: Center for War Studies, University of Southern Denmark.

Zhang, Q. (2026). China Is Not Unitary: Mapping the Diverse Actors Shaping China's Approach to AI Governance. In A. Nadibaidze & J. Lingevicius (Eds.), *Geopolitics of AI Governance: Actors, Norms and Trends* (pp. 21–27). Odense: Center for War Studies, University of Southern Denmark.

Cover image credit

Contents

Tables

Abbreviations

AI	Artificial Intelligence
BMFTR	German Federal Ministry of Research, Technology and Space
CAC	Cyberspace Administration of China
CISS	Centre For International Security and Strategy
DIESL	Digital Economic Security Lab
EC	European Commission
EDPS	European Data Protection Supervisor
EIF	European Investment Fund
EISA	European International Studies Association
EP	European Parliament
ERC	European Research Council
EU	European Union
FPIC	Free, Prior, and Informed Consent
GDPR	General Data Protection Regulation
GGE	Group of Governmental Experts
HCI	human-computer interaction
IHL	International Humanitarian Law
IR	International Relations
ITU	International Telecommunication Union
LAWS	lethal autonomous weapon systems
MFA	Ministry of Foreign Affairs
MIIT	Ministry of Industry and Information Technology
MND	Ministry of National Defence
MOST	Ministry of Science and Technology
NATO	North Atlantic Treaty Organization
OECD	Organisation for Economic Co-operation and Development
UK	United Kingdom
UN	United Nations
UNDP	UN Development Programme
US	United States
UX	user experience
VC	venture capital
WAICO	World Artificial Intelligence Cooperation Organization

Introduction

As artificial intelligence (AI) is increasingly integrated across various domains, actors including states, international institutions, civil society, and industry have launched a multitude of initiatives to address challenges and risks associated with these technologies. However, this governance landscape is complex, fragmented, and increasingly intertwined with ideologies, geopolitical interests, and identities.

The architecture of global AI governance is characterized by an interplay between the perceived pressure to outpace others in AI development on the one hand and norm-setting efforts on the other. Recent years have demonstrated that ambitions to govern the development and use of AI, whether through legislation, non-binding declarations, standards, or other means, are met with divergent positions and competition. These dynamics highlight the emergence of a new digital geopolitical space which deserves the attention of both analysts and policymakers.

This collective policy brief brings together a new generation of International Relations (IR) scholars who analyse the rapidly evolving complexity of actors, norms, and trends related to AI governance, broadly defined. It features thematic, conceptual, and geographical diversity, making it a timely addition to ongoing efforts in developing a comprehensive understanding of the spectrum of actors, policies, and tensions related to AI governance.

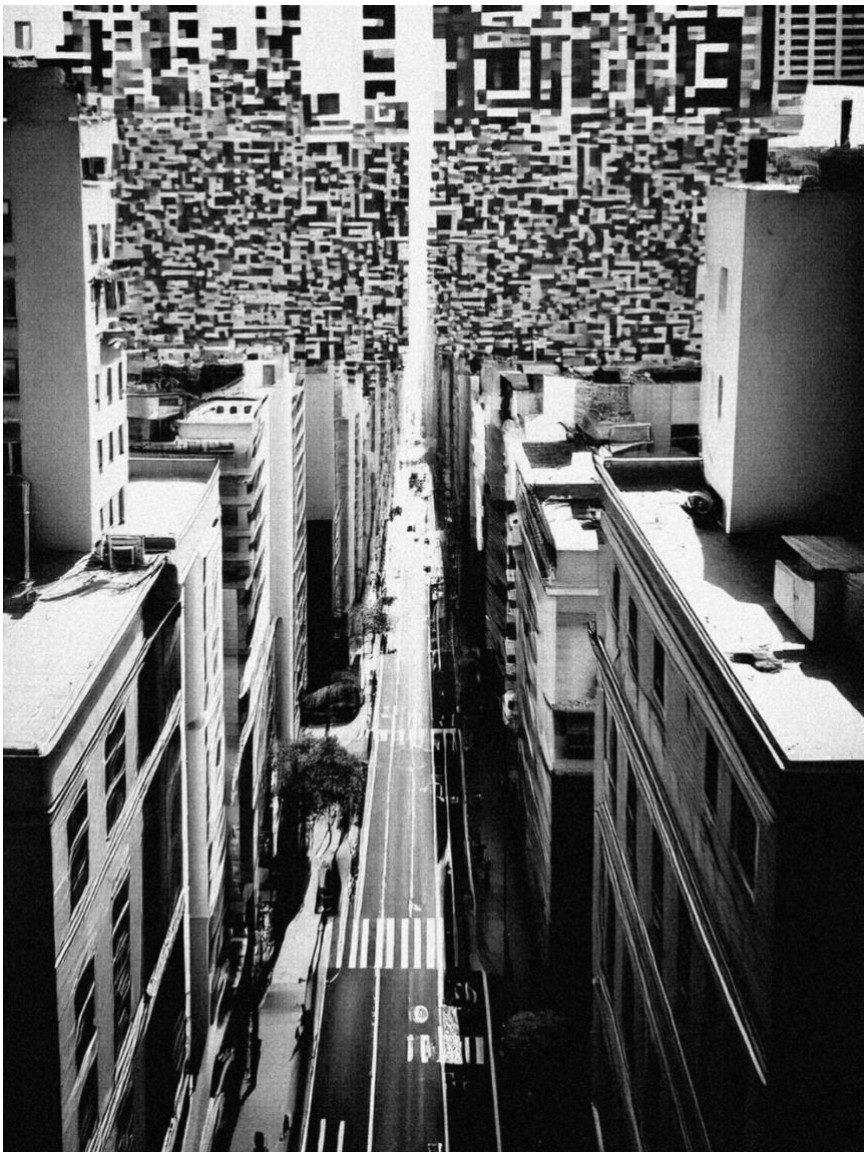
The collective policy brief includes seven contributions that are based on research presented and discussed at the Early Career Workshop “Geopolitics of AI Governance: Actors, Norms and Trends”, which took place on 25-26 August 2025 in Bologna, Italy as part of the 18th Pan-European Conference on International Relations hosted by the European International Studies Association (EISA).

This collective policy brief is intended for analysts and decision-makers involved in a range of AI governance issues. It may also be relevant to researchers across various disciplines beyond IR and security studies who are involved in debates on AI.

Each individual contribution includes policy recommendations, highlighting interests and inconsistencies that could be addressed by making AI governance more inclusive, accountable, and coordinated. Overall, the collective brief invites further conversations on various aspects of AI governance and demonstrates the need for further scrutiny and debate amid rapidly evolving political and technological landscapes.

Acknowledgements

The editors are grateful to the EISA for supporting the organization of the Early Career Workshop upon which this collective policy brief is based. The editors thank all workshop participants, as well as discussants Ingvild Bode and Fabio Cristiano, for providing valuable feedback and engaging in the constructive discussions that helped inspire the contributions to this policy brief. Finally, the editors extend their gratitude to Taja Tamkevičiūtė for supporting the production of this publication.



Beyond Prototypes and Products: The Influence of Defence Startups in Military AI Governance

Anna Nadibaidze
University of Southern Denmark, Denmark

Robin Vanderborght
University of Antwerp, Belgium

Executive summary

Defence-oriented startups are receiving record amounts of venture capital (VC) funding and an increasing number of government contracts to develop and supply AI technologies. Many startups, defined as privately owned companies focused on innovation and scalable growth, have also become prominent actors in debates on military AI governance. This contribution highlights two implications associated with the increased influence of defence AI startups. First, the growing role of startups signals a shift in the relationships between military actors and industry, with the reliance on military technologies supplied by the private sector reshaping political sovereignty and involving security risks. Second, beyond developing prototypes and supplying products, many startups are playing a central role in debates on governing AI in the military domain, shaping both legal and social norms related to military applications of AI. Based on these implications, this contribution proposes three main recommendations to policymakers from states seeking to acquire AI products from defence startups: 1) establish different types of relationships with startups; 2) critically assess narratives promoted by representatives of startups; and 3) ensure safeguards and avoid overreliance on limited suppliers.

Introduction

Policy discussions on the responsible development and use of AI in the military domain are considering what this means for the procurement of military AI capabilities.[1] The prominence of industry actors in developing AI technologies—whether hardware or

[1] Netta Goussac, "Responsible Behaviour in Military AI Starts with Responsible Procurement," *Stockholm International Peace Research Institute*, October 16, 2025, https://www.sipri.org/commentary/essay/2025/military-ai-responsible-procurement; Netta Goussac and Vincent Boulanin, *Responsible Procurement of Military Artificial Intelligence* (Stockholm International Peace Research Institute, 2026), https://www.sipri.org/publications/2026/other-publications/responsible-procurement-military-artificial-intelligence.

software—that defence organizations acquire makes it crucial to understand the evolving nexus between militaries and the private sector.[2]

While this connection is not new, current political dynamics reveal a perceived urgency among states around the globe to facilitate the acquisition of 'cutting-edge' AI-related technologies from the private sector. In many Western states, officials advocate for the reform of defence procurement processes, now often found too bureaucratic and slow, to be able to integrate new capabilities and technologies more quickly and keep up with the perceived global AI arms race.

At the same time, the private sector is not a unified actor: it is composed of different entities playing different roles in military AI development and governance. This contribution focuses on defence startups and unicorns (startups valued at over $1 billion). It argues that policymakers should scrutinize the broader implications of the increased reliance on startups' technologies, highlighting how these actors shape 1) new forms of relationships between the military and the private sector; and 2) new legal and social norms surrounding the use of AI in warfare.

The surge in defence AI investments and startups

As defence spending is increasing around the world, so are investments into AI technologies and their components. Recent and ongoing armed conflicts showcase whole ecosystems of infrastructures related to the use of AI-based weapon systems or decision-support systems,[3] including software, hardware, data, and cloud platforms to store data.

While many components of these ecosystems are supplied and maintained by Big Tech corporations such as Oracle, Microsoft, or Amazon, privately owned startups are increasingly emerging as key players in the field. With the support of VC funding, the number of startups seeking to develop AI technologies for security and defence has multiplied, especially in the United States (US), the United Kingdom (UK), Australia, and many European states.[4]

---

[2] Anna Nadibaidze, "Startups Envisioning Algorithmic Warfare: The Discourses of US Tech Companies in Defense AI," *Global Policy* 16, no. 3 (2025): 487–93, https://doi.org/10.1111/1758-5899.70047; Elke Schwarz, "Unicorns for Uniforms: On the Problematic Allure of VC Investments in Defence," *Opinio Juris*, September 18, 2024, https://opiniojuris.org/2024/09/18/unicorns-for-uniforms-on-the-problematic-allure-of-vc-investments-in-defence/; Elke Schwarz, "From Blitzkrieg to Blitzscaling: Assessing the Impact of Venture Capital Dynamics on Military Norms," *Finance and Society* (2025): 1–24, https://doi.org/10.1017/fas.2024.18.

[3] Anna Nadibaidze et al., *AI in Military Decision Support Systems: A Review of Developments and Debates* (Center for War Studies, 2024), https://www.autonorms.eu/ai-in-military-decision-support-systems-a-review-of-developments-and-debates/.

[4] Trevor Clawson, "As European Defense Investment Rises What Role Can Startups Play?" *Forbes*, October 16, 2025, https://www.forbes.com/sites/trevorclawson/2025/10/16/as-european-defense-investment-rises-what-role-can-startups-play/; Zoë Corbyn, "Move Fast, Kill Things: The Tech Startups Trying to Reinvent Defence with Silicon Valley Values," *The Guardian*, March 29, 2025, https://www.theguardian.com/world/2025/mar/29/move-fast-kill-things-the-tech-startups-trying-to-reinvent-defence-with-silicon-valley-values.

As Western governments increasingly view the acquisition of AI capabilities as a strategic priority, many are attempting to reform their procurement processes, with the intention to acquire technologies from startups. The funding landscape in military technologies is also changing. In 2025, funding for European defence startups rose to a record of $2 billion, with startups based in Germany and the UK receiving particularly high amounts of investments, and many companies growing more visible, such as Helsing (Germany), Quantum Systems (Germany), Tekever (Portugal/UK), Comand AI (France), and Systematic (Denmark).[5] Globally, in 2025 defence-focused startups received $48 billion, with 10 new unicorns being formed.[6]

Prominent US-based companies such as Anduril Industries, Shield AI, Epirus, or Skydio have obtained defence contracts for developing, supplying, and maintaining AI-based systems. For example, in September 2025 the Australian Department of Defence concluded an agreement with Anduril for "the delivery, maintenance and continued development" of the Ghost Shark underwater autonomous vehicle.[7] In the same month, the US Army awarded Anduril a contract to "equip every soldier with superhuman perception and decision-making capabilities—fusing the best of night vision, augmented reality, and AI into a single system", according to the company.[8]

Meanwhile in Europe, the startup Helsing was selected to supply AI-based software for the German Eurofighter, in collaboration with Saab Germany. The contract is reportedly worth €258 million.[9] These examples illustrate the increased influence of VC-funded startups in security and defence, which comes with broader political, legal, and social implications that warrant policymakers' scrutiny.

(Re)contextualizing relationships between states and startups

First, governments and military organizations risk increasing dependence on startups not only in terms of procuring AI technologies for defence, but also in terms of maintaining and updating them. This reliance on startups—and the private technology

[5] Kai Nicol-Schwarz, "AI Defense Booms in UK and Germany as New Wave of Billion-Dollar Startups Emerge," *CNBC*, December 11, 2025, https://www.cnbc.com/2025/12/11/ai-defense-boom-in-uk-and-germany-as-new-wave-of-companies-emerge.html.
[6] Alicia Park, "Thanks To Drones, China And Ukraine, A Record Number Of Military Startups Became Unicorns In 2025," *Forbes*, November 28, 2025, https://www.forbes.com/sites/aliciapark/2025/11/28/thanks-to-drones-china-and-ukraine-a-record-number-of-military-startups-became-unicorns-in-2025/.
[7] Mike Yeo, "Australia Signs Contract with Anduril for Ghost Shark Autonomous Underwater Vehicle," *Breaking Defense*, September 10, 2025, https://breakingdefense.com/2025/09/australia-signs-contract-with-anduril-for-ghost-shark-autonomous-underwater-vehicle/.
[8] Anduril Industries, "Anduril Awarded Contract to Redefine the Future of Mixed Reality," September 8, 2025, https://www.anduril.com/news/anduril-awarded-contract-to-redefine-the-future-of-mixed-reality.
[9] Helsing, "Helsing upgrades Eurofighter with Artificial Intelligence," November 19, 2025, https://helsing.ai/newsroom/helsing-upgrades-eurofighter-with-artificial-intelligence; Saab Press Centre, "Saab Receives Orders for Arexis System for German Eurofighter", November 14, 2025, https://www.saab.com/newsroom/press-releases/2025/saab-receives-orders-for-arexis-system-for-german-eurofighter.

sector more broadly—reflects a "shift in the character of armed conflict"[10] and, importantly, in how we conceptualize the phenomenon of political sovereignty, traditionally associated with a state's monopoly on means of using force.[11] What we see is an increasing dependence on privately-owned platforms for crucial security technologies, with financial and technical lock-ins as a result.[12]

Yet, VC-backed startups are not merely "neutral suppliers or patriotic agents of state policy".[13] They are driven by dynamics of venture capital, based on a business model that prioritizes speed and getting products on the market.[14] In the military context, this implies fast acquisition and integration over critical testing of AI-based systems to ensure that they are used to support the exercise of human judgement, rather than undermine it, and that these systems are appropriate to the intended context of use and not just adopted for the sake of integrating AI.

For military organizations seeking to use AI-based systems in a way that strengthens human agency, overreliance on startups or private sector actors might involve security risks. Software design and development is a crucial stage in the context of military applications of AI, especially those related to targeting in weapon systems or decision-support systems.

Relying on startups for software design, development and maintenance, especially when intended users of AI systems are not involved a lot or at all, increases risks of severe malfunctions.[15] Operator involvement is particularly important to test various instances of human-machine interaction, i.e., interactions between intended users and systems, especially in a network of systems.[16] Therefore, dependence on startups with financial and technical lock-ins as a result involves both political risks (weakened sovereignty) and operational implications (risks of malfunctions) that policymakers should consider.

---

[10] Emily Bienvenue et al., "Private Tech Companies, the State, and the New Character of War," *Carnegie Endowment for International Peace*, December 1, 2025, https://carnegieendowment.org/research/2025/12/ukraine-war-tech-companies?lang=en.
[11] Rupert Barrett-Taylor and Matthew Ford, "Eroding Sovereignty in the Age of 'War as a Service,'" *Opinio Juris*, November 3, 2025, https://opiniojuris.org/2025/11/03/eroding-sovereignty-in-the-age-of-war-as-a-service.
[12] Marijn Hoijtink and Jasper van der Kist, "Platforms on the Frontline: The Rise of the Platform Model in Defense Tech," *Opinio Juris*, February 11, 2025, https://opiniojuris.org/2025/02/11/platforms-on-the-frontline-the-rise-of-the-platform-model-in-defense-tech/.
[13] Bienvenue et al., "Private Tech Companies, the State, and the New Character of War."
[14] Elke Schwarz, "When War Becomes a Tech Product: How Silicon Valley Logics Are Reshaping Military AI - Untold," *Untold Mag*, June 22, 2025, https://untoldmag.org/when-war-becomes-a-tech-product-how-silicon-valley-logics-are-reshaping-military-ai/; Elke Schwarz, "Tech, Venture Capital and the Hype of War," *Tech Policy Press*, January 22, 2026, https://techpolicy.press/tech-venture-capital-and-the-hype-of-war.
[15] Jeffrey Ding, "Machine Failing: How Systems Acquisition and Software Development Flaws Contribute to Military Accidents," *Texas National Security Review* 8, no. 1 (2024): 9–29, https://doi.org/10.26153/tsw/58064.
[16] Networks of systems appear to be the priorities for many startups. See Systematic, "Systematic and Helsing Join Forces for Sovereign Control of Drone Swarms," September 10, 2025, https://systematic.com/int/industries/defence/news-knowledge/news/europe-s-tech-leaders-join-forces-for-sovereign-control-of-drone-swarms/.

The role of startups in military AI governance

A second key aspect of the increased influence of startups is their political role in the governance of AI in the military domain. As central actors in the development of military applications of AI, they can shape the interpretation of international humanitarian law (IHL, enshrined in legal obligations) and social norms (what counts as appropriate behaviour).[17]

Design choices made by startups in the development of AI systems can have far-reaching implications, especially when it comes to IHL.[18] For example, military personnel's capability to engage in the legal judgements necessary for complying with IHL principles—such as distinction, proportionality, and precaution—may be affected by personnel's interactions with AI-based decision-support systems, including as a result of the systems' interface design.[19]

Moreover, many startups are prominently represented in debates on AI in the military domain taking place in global forums (e.g., the Responsible AI in the Military Domain summits), domestic policy discussions, defence exhibitions, the media landscape, and social media, among others. This provides representatives of defence AI startups the opportunity to influence what is considered the appropriate and responsible development and use of AI in the military domain.

They reproduce specific narratives and tropes about military applications of AI, including portraying AI technologies as making warfare more efficient, precise, and inherently better at limiting collateral damage or consequences affecting civilians.[20] But evidence from the wars in Gaza and Ukraine, where military AI capabilities are

[17] Ingvild Bode, *Emerging Norms around Military Applications of AI: The Case of Human Control*, GC REAIM Expert Policy Note Series (The Hague Centre for Strategic Studies, 2025), https://hcss.nl/wp-content/uploads/2025/05/Bode-1.pdf.

[18] Yiokasti Mouratidi, "Armed Groups and International Law - Beyond Compliance Symposium: Before Compliance – Ex-Ante Decision Making in the Design of Military AI Capabilities and the Need to Unravel the Private Technology Sector's Role," *Armed Groups and International Law*, September 23, 2025, https://www.armedgroups-internationallaw.org/2025/09/23/beyond-compliance-consortium-before-compliance-ex-ante-decision-making-in-the-design-of-military-ai-capabilities-and-the-need-to-unravel-the-private-technology-sectors-role/.

[19] Jessica Dorsey and Marta Bo, "AI-Enabled Decision-Support Systems in the Joint Targeting Cycle: Legal Challenges, Risks, and the Human(e) Dimension," *International Law Studies* 107 (2026), https://digital-commons.usnwc.edu/ils/vol107/iss1/7/; Jessica Dorsey, "The Erosion of Human(e) Judgement in Targeting? Quantification Logics, AI-Enabled Decision Support Systems and Proportionality Assessments in IHL," *International Review of the Red Cross* (2026): 1–31, https://doi.org/10.1017/S1816383125100969.

[20] Robin Vanderborght and Anna Nadibaidze, "Demonstrating the Future of War: Tech Companies and Claims of Epistemic Authority on Military AI," *Opinio Juris*, November 19, 2025, https://opiniojuris.org/2025/11/19/demonstrating-the-future-of-war-tech-companies-and-claims-of-epistemic-authority-on-military-ai/; Robin Vanderborght and Anna Nadibaidze, "Military Demonstrations as Digital Spectacles: How Virtual Presentations of AI Decision-Support Systems Shape Perceptions of War and Security," *European Journal of International Security* (2025): 1–20, https://doi.org/10.1017/eis.2025.10015.

reportedly playing a key role,[21] demonstrates that warfare is far from clean, precise or limited.[22]

Nevertheless, executives routinely depict the products they sell—and with which they earn their profits—as the morally 'right' technologies to use for military targeting. For example, Palmer Luckey, the founder of Anduril, claimed that

> when it comes to life and death decision-making, I think that it is too morally fraught an area, it is too critical of an area, to not apply the best technology available to you, regardless of what it is… If you're talking about killing people, you need to be minimizing the amount of collateral damage. You need to be as certain as you can in anything that you do.[23]

While the available evidence seems to counter the argument that military AI systems used in targeting decision-support are providing 'certainty' and reducing collateral damage to civilians,[24] the constructed narrative risks promoting various sorts of military applications of AI as unconditionally permissible and desirable. This, in turn, is likely to undermine the broad public support necessary to build a robust military AI governance framework which can limit the risks of these applications.

This narrative is further entrenched by defence AI startups' regular demonstrations of their products, such as AI-based decision-support systems or (semi-)autonomous drones.[25] Through widely watched and shared social media videos and digital creations, these demonstrations create a visual narrative which reinforces the perception that AI-enabled warfare, where machines and software programs can independently seek, identify and even attack targets, will be limited, clean and errorproof. The absence of civilians, collateral damage or large-scale infrastructural destruction in these videos strengthens the image of AI-enabled war as a morally and strategically justified practice. Consequently, important deliberations regarding responsibility and accountability might move to the background, while the threshold for starting war could become lower for policymakers and the general public.

---

[21] Elizabeth Dwoskin, "Israel Built an 'AI Factory' for War. It Unleashed It in Gaza," *The Washington Post*, December 29, 2024, https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/; Vera Bergengruen, "How Tech Giants Turned Ukraine into an AI War Lab," *TIME*, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/.

[22] Samuel Sigal, "Some Say AI Will Make War More Humane. Israel's War in Gaza Shows the Opposite.," *Vox*, May 8, 2024, https://www.vox.com/future-perfect/24151437/ai-israel-gaza-war-hamas-artificial-intelligence.

[23] Lauren Edmonds, "Anduril's Palmer Luckey Makes an Ethical Case for Using AI in War: 'There Is No Moral High Ground in Using Inferior Technology'," *Business Insider*, December 7, 2025, https://www.businessinsider.com/anduril-palmer-luckey-ai-war-conflict-defense-tech-startups-military-2025-12.

[24] Yuval Abraham, "IDF Database Suggests 83% of Gaza Dead Were Civilians," *+972 Magazine*, August 21, 2025, https://www.972mag.com/israeli-intelligence-database-83-percent-civilians-militants/; Lauren Gould et al., "Gaza War: Artificial Intelligence is Changing the Speed of Targeting and Scale of Civilian Harm in Unprecedented Ways," *The Conversation*, April 23, 2024, https://doi.org/10.64628/AB.4yutwax4s.

[25] Vanderborght and Nadibaidze, "Demonstrating the Future of War"; Vanderborght and Nadibaidze, "Military Demonstrations as Digital Spectacles."

In the name of increasing speed and reducing bureaucracy, VC investors and defence AI executives, especially in the US, suggest overhauling traditional military acquisition and procurement processes. Yet, these processes are in place to ensure the purchase of safe and functional military equipment.[26] Integrating the VC logic and Silicon Valley mentality, which is essentially based on hyping up unfinished products and 'moving fast and breaking things' into the military domain by disrupting these procedures and safeguards, risks the spread of unsafe and ill-functioning weaponry, equipment, or software. In addition to potentially increasing harm to civilians and civilian infrastructure, defence startup products that are insufficiently tested or attuned to the appropriate capabilities or assignment involve considerable security challenges.

Recommendations

Based on the implications of startups' increased influence and role in military AI governance debates, this contribution issues the following recommendations to policymakers in states seeking to acquire AI products from defence startups:

1. **Establish different forms of engagement with defence AI-focused startups, which are appropriate to the capabilities and the contexts.** This involves paying attention to the procurement and acquisition of AI technologies from the private sector, including how these processes are changing in the AI context; investing efforts into understanding different types of involvement with startups and other actors; and the formats this can take.

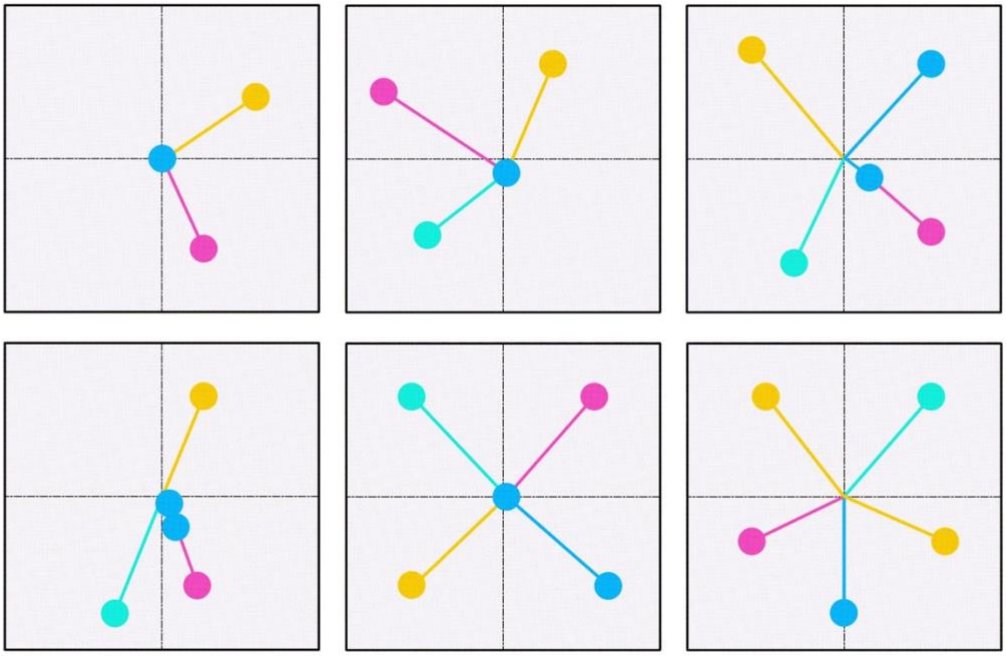
2. **Critically assess narratives promoted by representatives of startups in the governance debate on military applications of AI**. Policymakers should ensure that their organizations' definitions of risks and priorities align with those of startups they seek to acquire technologies from, paying critical attention to these startups' role in AI governance. Policymakers should consider that defence startups visually demonstrate their products in spectacular and hyperbolic fashion to attract funding, often downplaying potential risks.

3. **Ensure safeguards and avoid overreliance on particular suppliers.** When possible, policymakers should prioritize maintaining a diverse, competitive ecosystem of suppliers of various elements of AI systems.[27] Policymakers should maintain systematic acquisition and procurement procedures, even when pressured to overhaul many of these safeguards in the name of increasing speed and efficiency.

[26] Zena Assaad and Jessica Dorsey, "Designing Lawful Military AI: Technical and Legal Reflections on Decision-Support and Autonomous Weapon Systems," *Perry World House*, November 24, 2025, https://perryworldhouse.upenn.edu/news-and-insight/designing-lawful-military-ai-technical-and-legal-reflections-on-decision-support-and-autonomous-weapon-systems/.
[27] Anna Knack et al., *Applying AI to Strategic Warning* (Centre for Emerging Technology and Security, 2025), https://cetas.turing.ac.uk/publications/applying-ai-strategic-warning.

Acknowledgements

Anna Nadibaidze's contribution was supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 852123, the AutoNorms project) and the Independent Research Fund Denmark (grant ID 3119-00023B, the HuMach project).



The Geopolitics of Human-Centred AI at EU Borders

Stefka Schmid
Aalto University, Finland

Executive summary

The geopolitical dimension of AI innovation has become more apparent. The European Union (EU)'s adoption of technologies in critical domains such as border control, as its approach to AI governance, are embedded in this geopolitical context. This contribution argues that the increased pressure to adopt AI technologies at the EU's external borders risks exacerbating challenges in relation to data autonomy, techno-solutionism, and vendor lock-in. Based on an analysis of how Frontex-supported Horizon research projects envision human-AI interaction in EU border control, this contribution issues three recommendations to European policymakers and applied research communities. First, these projects' human-centred design matches the EU branding of trustworthy AI and focuses on the operators' needs. However, their underlying aim is to integrate AI successfully into teamwork, even at the cost of compliance with data protection or the autonomy of individuals crossing the EU's external borders. Second, a more open, socio-technical understanding of innovation and iterative design and development is needed. Third, AI should not be applied without considering economic interests and the risk of vendor lock-in in critical contexts of use.

Introduction

The geopolitical turn in AI innovation manifests itself across different contexts of application, including critical domains such as border control. Amid US-Sino competition and increasing geopolitical tensions, the EU tries to navigate AI innovation and dependencies on foreign Big Tech companies. The EU is committed to adopt AI across various contexts of application, including critical infrastructure or law enforcement. For the sake of 'border security', EU border agency Frontex supports applied research that aims to implement AI into border control, customs, identity and fraud detection, communication between (coastal) authorities, and detection of submarine threats. At the same time, the EU brands its approach to AI as 'human-centric', building upon the concepts of trustworthy and ethical AI.

This contribution explores the tensions between the pressure to adopt AI and the commitment to serve human needs in the EU's border control policies. It draws on an

explorative analysis of eight border security projects funded by Frontex within the framework of the EU's Horizon 2023 programme,[1] focusing on how these projects envision human-centred AI to be implemented in practice at EU borders.

The contribution argues that the geopolitics of AI are characterized by governance at the cost of ethics and safety, perception of AI as a solution to diverse problems, and the entanglement of security and economy rationales.[2] Applied research projects in the field of border control reflect these dynamics, which themselves entail different challenges that arise in practice, i.e., in the design, development, and implementation of AI. These challenges are: constrained privacy and data autonomy, an overly optimistic understanding of AI, and the risk of vendor lock-in and dependencies. To address these challenges, the contribution issues three main recommendations to EU policymakers and research communities, namely (1) comply with existing EU data regulation and inclusion of value-sensitive design approaches, (2) foster a more open, socio-technical understanding of design and development, and (3) prioritize EU-owned, open-source solutions.

Human-AI collaboration in border control

Frontex-supported Horizon projects appear to align with the EU's broader agenda of a more ethical, human-centric approach to AI adoption. More concretely, this requires a focus on the needs and wants of end-users.[3] In border control, these are "primarily Customs, Police, and Airport Operators".[4] Designing technology guided by the needs of its end-users has clear benefits, as otherwise technology could potentially cause failures or accidents and therefore would be unusable or unnecessary. Thus, human-centred design focuses on usability as a foundational design characteristic. Usability entails that technology is effective, efficient, and satisfactory, with the latter pointing out the importance of good user experience (UX).[5]

Certain tasks in border control, whether routine or not, are supposed to be carried out in collaboration with AI, aiming at "reducing the need for physical inspections" or the "complete automation" of some duties.[6] This should give human staff the opportunity to allocate their resources, e.g., to "focus only on pieces marked as suspicious" in

[1] Frontex, "EU Research: New EU-funded Border Security Projects," March 26, 2024, https://www.frontex.europa.eu/innovation/eu-research/news-and-events/new-eu-funded-border-security-projects-AQlKy3.
[2] Stefka Schmid et al., "Arms Race or Innovation Race? Geopolitical AI Development," *Geopolitics,* 30, no. 4 (2025): 1908, https://doi.org/10.1080/14650045.2025.2456019.
[3] CONNECTOR, "About CONNECTOR," n.d., accessed February 1, 2026, https://www.connector-project.eu/about.
[4] "BAG-INTEL, *D2.1: End Users, Legal and Ethical Requirements (First Version)* (2024), https://bag-intel.eu/wp-content/uploads/sites/105/2024/11/BAG-INTEL-Deliverable-D2.1-End_users_legal_and_ethical_requirements.pdf.
[5] International Organization for Standardization, "ISO 9241-11:2018(en) Ergonomics of Human-System Interaction — Part 11: Usability: Definitions and Concepts," 2018, https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en.
[6] METEOR, "About METEOR," n.d., accessed February 1, 2026, https://www.meteor-project.eu/about.

baggage control.[7] Further, putting emphasis on increased efficiency, the BAG-INTEL project states that it aims for "supporting smarter, safer, and more efficient border management through AI-driven innovation".[8] Other relevant features of AI applications in border management include accuracy, information quality, as well as interoperability and flexibility,[9] all understood to contribute to usable AI in border control.

As indicated in border control research projects, the vision of human-centred, usable AI reiterates the EU's approach of trustworthy and ethical AI. However, as human-computer interaction (HCI) scholarship has noted, usability is a broad label and has been used for the justification of all kinds of technology.[10] With an increased geopolitical understanding of AI innovation, governance is carried out at the cost of ethics and safety, while AI is seen as a solution to almost any problem, and security and economic concerns are intertwined. These dynamics have an impact on how usable AI is realized in practice. While Horizon research projects share a rather future-oriented view of how AI might be implemented in border control, they serve as points of reference and give insight into these potential challenges.

AI as a useful tool? Challenges arising

The geopolitics of AI means that the EU's governance approach increasingly prioritizes efficiency over safety and ethics. Regarding AI in border control, this entails that requirements of ethical AI such as privacy and data autonomy (individuals' ownership of their data) are sacrificed for the need of AI training data. The vision of usable AI includes efficiency as well as privacy, but, while presented alongside each other, there is a trade-off in practice.

The cost of data autonomy

Data is the foundation of AI adoption and allows for the application of data analytics and detection models.[11] Therefore, vast amounts of data, including individuals' personal data, are collected and processed. Aligning with the idea of human-centred design, various Frontex-supported projects emphasize privacy.[12] The demand for

[7] BAG-INTEL, "Background and Scope," n.d., accessed February 1, 2026, https://bag-intel.eu/background-and-scope/.
[8] BAG-INTEL, "BAG-INTEL Showcases AI Solutions for Smarter Border Management at I-SEAMORE Webinar," April 16, 2025, https://bag-intel.eu/2025/04/16/bag-intel-showcases-ai-solutions-for-smarter-border-management-at-i-seamore-webinar/.
[9] CONNECTOR, "Our Innovations," n.d., accessed February 1, 2026, https://www.connector-project.eu/our-services; European Commission, "Interoperable Applications Suite to Enhance European Identity and Document Security and Fraud Detection," n.d., accessed February 1, 2026, https://cordis.europa.eu/project/id/101121280; BAG-INTEL, "Background and Scope."
[10] Paul Dourish, "User Experience as Legitimacy Trap," *Interactions*, 26, no. 6 (2019): 47–49, https://doi.org/10.1145/3358908.
[11] European Commission, "E-commerce Security and Countering Illicit Transactions," July 19, 2024, https://home-affairs.ec.europa.eu/news/e-commerce-security-and-countering-illicit-transactions-2024-07-19_en.
[12] European Commission, "Interoperable Applications Suite to Enhance European Identity and Document Security and Fraud Detection."

privacy-enhancing technologies "becomes even more critical as AI adoption accelerates and the demand for secure, ethical and trustworthy data practices intensifies".[13] In practice, however, Frontex's "move to the cloud"—crucial for AI adoption—has been reprimanded by the European Data Protection Supervisor (EDPS) because of the lack of "proper data protection assessment"[14] and failure "to observe the principles of lawfulness and data minimisation".[15]

Further, while Frontex-supported research projects point out the "goal of General Data Protection Regulation (GDPR) compliance", they put emphasis on the "preservation of *citizens*' privacy".[16] With regard to non-EU citizens who try to enter the EU, both activists and scholars have voiced criticism over the authorities pressuring individuals to access their personal devices, such as smartphones.[17] When migration is forced, people often appear in precarious situations when their data autonomy is at stake.

Building on HCI literature, it becomes clear that there are different paradigms of design approaches.[18] With the geopolitical turn of AI innovation, applied research primarily builds on solutionist, deterministic approaches, and disregards open, socio-technical frameworks.

Deterministic design and development

In EU border control, research projects reflect a narrow view of technology. Frequently, such applied research builds on deterministic understandings, more specifically, technological solutionism, i.e., the idea that technology can ultimately fix any (social) problem.[19] Through applied research, AI is understood to be systematically designed and developed—and ultimately result in solutions for different border control purposes, including the protection of critical infrastructures, fighting drug trafficking, illegal fishing or immigration[20] and airport security checks.[21] Instances in which projects refer to

[13] Annalisa Triggiano and Daisy Romanini, "Policy Brief - AI, Data Governance and Cloud Cybersecurity in Maritime Surveillance", *Zenodo*, April 28, 2025, https://doi.org/10.5281/zenodo.15425760.
[14] Micaela del Monte and Katrien Luyten, *European Parliament Scrutiny of Frontex* (European Parliamentary Research Service, 2023), https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698816/EPRS_BRI(2021)698816_EN.pdf.
[15] European Data Protection Board, "2022 Coordinated Enforcement Action Use of Cloud-Based Services by the Public Sector," January 17, 2023, https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf.
[16] European Commission, "SafeTravellers: Secure and Frictionless Identity for EU and Third Country National Citizens," n.d., accessed February 1, 2026, emphasis added, https://cordis.europa.eu/project/id/101121269/reporting.
[17] Ivan Josipovic, "What Can Data Justice Mean for Asylum Governance? The Case of Smartphone Data Extraction in Germany," *Journal of Refugee Studies* 36, no. 3 (2023): 543, https://doi.org/10.1093/jrs/fead049.
[18] Shaowen Bardzell, "Feminist HCI: Taking Stock and Outlining an Agenda for Design," *CHI '10: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2010): 1302, https://doi.org/10.1145/1753326.1753521.
[19] Jay Cunningham et al., "On the Grounds of Solutionism: Ontologies of Blackness and HCI," *ACM Transactions on Computer-Human Interaction* 30, no. 20 (2023): 4, https://doi.org/10.1145/3557890.
[20] CISE-ALERT, "Join the CISE-ALERT VIP DAYS in Rome!" May 30, 2024, https://cise-alert.eu/node/62.
[21] BAG-INTEL, "Use Cases," n.d., accessed February 1, 2026, https://bag-intel.eu/use-cases/.

different procedural steps, including integration, demonstration, and validation,[22] do not pay much attention towards questions of how to adequately[23] evaluate and assess technologies in relation to regulation and real-world environments.

Besides the predominant solutionist view, research projects rarely reflect a more open, less deterministic understanding of AI, indicating that successful application is "not granted".[24] In these rare instances, they consider that design is a socio-technical process and relate to participatory design approaches and co-design principles.[25]

Further, as critical HCI scholarship has noted,[26] economic rationales are prevalent in AI innovation, with designers and developers traditionally being employed at tech companies. This might not only pose a problem considering the actual achievement of long-term goals, but also create dependencies in critical domains through vendor lock-in.

Vendor lock-in in security domains

In border control, involved actors are diverse and projects regularly build on industry partnerships. As in other domains, research projects on border control rely on use case trials.[27] In live demonstrations, border control practitioners can "interact with system developers and researchers".[28] Border control is becoming a market, with tech companies offering experts and "current state-of-the-art technologies".[29]

In some projects, technological adoption becomes a way to "industrial competitiveness",[30] again indicating an economic rationale. As can be seen in other critical domains such as local law enforcement or the military, it is important for political and academic actors to pay attention to diverging stakeholder interests and the risk of vendor lock-in, which creates dependencies on Big Tech companies and their home governments.

---

[22] European Commission, "Underwater Security," n.d., accessed February 1, 2026, https://cordis.europa.eu/project/id/101121288/results.

[23] Alan Hevner et al., "Design Science in Information Systems Research," *MIS Quarterly* 28, no. 1 (2004): 77, 100, https://doi.org/10.2307/25148625; Steven Smithson and Rudy Hirschheim, "Analysing Information Systems Evaluation: Another Look at an Old Problem," *European Journal of Information Systems* 7, no. 3 (1998): 158, https://doi.org/10.1057/palgrave.ejis.3000304.

[24] BAG-INTEL, "65th ESReDA Seminar From Risk Imagination to Safety Intervention – Managing Risks with Knowledge," November 15, 2024, https://bag-intel.eu/event/65th-esreda-seminar-from-risk-imagination-to-safety-intervention-managing-risks-with-knowledge/.

[25] BAG-INTEL, "65th ESReDA Seminar From Risk Imagination to Safety Intervention"; BAG-INTEL, "Use Cases."

[26] Meredith Whittaker, "The Steep Cost of Capture," *Interactions*, 28, no. 6 (2021): 51, https://doi.org/10.1145/3488666.

[27] European Commission, "CustOms exteNded iNteroperablE Common informaTiOn shaRing environment," n.d., accessed February 1, 2026, https://cordis.europa.eu/project/id/101121271; SafeTravellers, "Methodology," n.d., accessed February 1, 2026, https://safetravellers-project.eu/about/methodology/.

[28] RISE-SD, "Research and Innovation Symposium for European SECURITY and Defense 2026," n.d., accessed February 1, 2026, https://rise-sd.net/.

[29] UnderSec, "Consortium," n.d., accessed February 1, 2026, https://www.undersec-project.eu/consortium.

[30] Antonis Sapountzis, "SMAUG - Impact Master Plan," *Zenodo*, March 28, 2024, https://doi.org/10.5281/zenodo.10986724.

Currently, it is not entirely clear to what extent AI has already been applied in EU border control. Combined with EU policies such as the AI Act—which only partially considers applications in border and migration control as "high-risk"[31]—Frontex, political, academic, and industry partners reiterate the motivation to integrate AI into border control settings. The involvement of Big Tech and defence companies indicates the idea that AI models are applicable across contexts as the

> border security market is witnessing an influx of collaborations between established defence contractors, technology companies, and AI startups [and] [...] companies such as NVIDIA, Microsoft, and IBM provide the computing infrastructure and AI algorithms necessary for large scale data processing.[32]

While defence and border operations might share command and control frameworks[33] and the broader goal of "situational awareness",[34] these domains should not be equated. AI is not as easily transferable from one context to another because the "context of use",[35] defined by the physical, organizational setting or specific design goals, is highly important.

Conclusion

Today, geopolitics are not only carried out on the battlefield. States, in partnership with industry, foster research and development for both military and civilian application contexts. Border control, a domain declared relevant to European security and where consequences of human-AI interaction are highly impactful, increasingly becomes a site of geopolitics. Arguably, related dynamics, such as prioritization of speed and efficiency over ethics, orientation towards a solutionist understanding of AI, and intertwined security and economic concerns, have an impact on how the EU implements AI in security domains, including border control. Answering to arising challenges, EU policymakers and research communities should adopt measures that contribute to slowing down the global "AI race".[36]

---

[31] Evelien Brouwer, "EU's AI Act and Migration Control. Shortcomings in Safeguarding Fundamental Rights," *Verfassungsblog*, December 12, 2024, https://verfassungsblog.de/eus-ai-act-and-migration-control-shortcomings-in-safeguarding-fundamental-rights/.
[32] Market and Markets, "AI Impact Analysis on Border Security Industry", n.d., accessed December 16, 2025, https://www.marketsandmarkets.com/ResearchInsight/ai-impact-analysis-on-border-security-industry.asp.
[33] Ibid.
[34] CONNECTOR, "Our Innovations"; Ridley Jones et al., "Construction of Shared Situational Awareness in Traffic Management," *Proceedings of the ACM Human-Computer Interaction* 5, issue CSCW1, no. 54 (2021): 3, https://doi.org/10.1145/3449128.
[35] Interaction Design Foundation, "Contexts of Use", n.d., accessed December 16, 2025, https://www.interaction-design.org/literature/topics/contexts-of-use?srsltid=AfmBOopsvL-GYCgYijMFHnEQG4DoG7tt1SAkWfgG6qfsE1rus7-TcnP0.
[36] Schmid et al., "Arms Race or Innovation Race? Geopolitical AI Development," 1908.

Recommendations

This contribution issues three main policy recommendations to EU policymakers and research communities.

1. While the paradigm of human-centred design fits the EU branding of trustworthy and ethical AI, it should be clear that design approaches focus on utility and usability for operators, ultimately aiming at the integration of AI into teamwork. Whereas a human-centred approach is generally favourable, policymakers should critically assess to which degree AI adoption in border control, building on big data and cloud computing, is **compliant with existing EU data regulation**. Further, under the current premise of **value-sensitive design**, applied research communities should also emphasize approaches to **privacy and data autonomy**.

2. **Research communities should foster a more non-linear, social understanding of innovation to avoid the application of less ideal AI models**. While some research already puts emphasis on socio-technical understandings of design and development, it is important that projects go beyond branding, rely on social and legal perspectives for assessment, and use resources for evaluation and feedback cycles. This applies particularly when the loss of human lives is more likely (e.g., surveillance of external coastal borders vs. cargo screening).

3. Although EU policies emphasize the criticality of border control, actors of the "AI ecosystem"[37] may aim to transfer an AI application from one environment to another. **Here, policymakers should pay attention to the specific contexts of use in border control**, which might not require the adoption of AI or make transfers of AI models from one context to another less easy as it may seem. From an EU perspective, **the risk of vendor lock-in and dependencies could be decreased with public, open-source technology**.

Acknowledgements

This work has been supported by the German Federal Ministry of Research, Technology and Space (BMFTR) as part of TraCe "Regional Research Center Transformations of Political Violence" (01UG2203E).

[37] Burcu Kilic, *AI, Innovation and the Public Good: A New Policy Playbook*, CIGI Papers no. 318 (Centre for International Governance Innovation, 2025): 6, https://www.cigionline.org/publications/ai-innovation-and-the-public-good-a-new-policy-playbook/.

Anton Grabolle / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

China Is Not Unitary: Mapping the Diverse Actors Shaping China's Approach to AI Governance

Qiaochu Zhang
European University Institute, Italy

Executive summary

This contribution identifies three key domains shaping China's approach to AI governance—security, technology, and diplomacy—and maps the diverse key actors operating within each domain. These actors hold varied, though not necessarily contradictory, positions on AI governance. By moving beyond the assumption that China acts as a single, unified actor, the contribution offers two main insights. First, cooperation with China is expected to be more productive in the civilian domain than in the military domain. Second, the contribution recommends that international engagement should not rely solely on government-to-government channels. Complementary outreach to think tanks and technology companies may be beneficial, as these actors are becoming more active and can contribute to shaping regulatory discussions. Nevertheless, their influence remains constrained by the overarching structures of China's authoritarian political system.

Introduction

Despite the rapid development of AI technologies and their potentially far-reaching impact on societies, a persistent gap remains in efforts to establish an international framework to govern them.[1] To help address this pressing issue, this contribution examines China's approach to governing AI. As China seeks to position itself as a leading developer of AI and an influential actor in global governance, understanding its regulatory strategy has become essential. This contribution moves beyond the assumption that China operates as a unitary actor with a coherent and uniform position on AI governance. Instead, it examines the practices of sub-state actors and shows that diverse approaches to AI governance are emerging within China.[2]

[1] Ingvild Bode et al., "Prospects for the Global Governance of Autonomous Weapons: Comparing Chinese, Russian, and US Practices," *Ethics and Information Technology* 25, no. 5 (2023), https://doi.org/10.1007/s10676-023-09678-x.
[2] Qiaochu Zhang, "Different Fields, Different Appropriateness? Unpacking Emerging Normativity in China's AI Governance," *Cooperation and Conflict* (2025), https://doi.org/10.1177/00108367251383688.

The contribution proceeds as follows. First, it identifies three core domains that shape China's AI governance landscape—security, technology, and diplomacy—and maps the key actors involved in each. It outlines their respective preferences and positions on how AI should be governed. Building on these empirical insights, the contribution concludes with two policy implications and recommendations for international observers and stakeholders seeking to understand China's approach to AI governance, particularly governments and civil society actors aiming to contribute to the development of a global framework for governing AI technologies.

The first concerns the types of global AI governance initiatives that China is more likely to support or oppose. The second suggests opportunities for coalition-building with specific Chinese actors to influence China's broader stance on AI governance. Together, these insights provide a more nuanced understanding of China's official positions—which are often obscured by abstract and ambiguous public rhetoric—and, crucially, point towards more targeted and constructive avenues for engaging with China in the development of global AI governance initiatives.

The three domains of Chinese AI governance

The security domain

The security domain of AI governance in China is shaped primarily by the objective of safeguarding national security. However, it should be noted that China's interpretation of national security differs from Western understandings. In the Chinese context, national security is closely tied to political security—often described as regime security—which centres on preserving the authority and stability of the party-state.[3] In this sense, national security is understood not only as protecting the state's survival but also as ensuring the continued dominance and legitimacy of the ruling regime. China has rarely explicitly identified the sources of threats to its national security. However, official documents—such as the 2025 Defence White Paper, which states that "a certain country seeks absolute strategic superiority by constantly expanding its armaments"—are widely interpreted as referring to the US.[4]

In responding to perceived national security threats, particularly those associated with the US, two actors stand out due to the division between civilian and military uses of AI technologies: the Cyberspace Administration of China (CAC) and the Ministry of National Defence (MND). The CAC focuses on regulating AI-generated content that

[3] Jonna Nyman, "Towards a Global Security Studies: What Can Looking at China Tell Us about the Concept of Security?" *European Journal of International Relations* 29, no. 3 (2023): 673–97, https://doi.org/10.1177/13540661231176990.
[4] Ministry of Foreign Affairs of the People's Republic of China, "China Releases White Paper on Arms Control in New Era," November 27, 2025, https://www.fmprc.gov.cn/mfa_eng/xw/wjbxw/202511/t20251127_11761653.html; Sabine Mokry, "The PRC's Expanding Arms Control Agenda," *Jamestown*, November 12, 2025, https://jamestown.org/the-prcs-expanding-arms-control-agenda/.

could undermine political security by circulating information perceived as inconsistent with the Chinese Communist Party's official ideology. The MND, by contrast, focuses on the military applications of AI and plays a leading role in accelerating the development of AI technologies within the defence sector.

Although both actors are situated in the security domain, they adopt different positions on AI's implications for national security. The CAC views AI technologies—particularly AI-generated content—as potential threats to political security that necessitate strict regulation. Accordingly, it has issued three major regulations: the *Regulations on the Management of Algorithmic Recommendation* (2021), the *Regulations on the Management of Deep Synthesis* (2022), and the *Measures for the Management of Generative AI Services* (2023). In contrast, the MND views AI development as essential for gaining a strategic advantage in future warfare and strengthening national security. Specifically, despite China's rapid technological progress, the MND continues to perceive a gap with the US in key areas of military AI capability.[5] This perceived shortfall reinforces its commitment to advancing the development and deployment of AI in weapons systems and other military platforms.

The technology domain

In the technology domain, two governmental actors play central roles: the Ministry of Science and Technology (MOST) and the Ministry of Industry and Information Technology (MIIT). The two actors adopt broadly aligned positions on AI governance. Their positions include two interrelated aspects. First, they both emphasize that governance should not impede technological progress, arguing that AI can drive economic growth and, in some cases, provide technological solutions to social challenges.

Second, they recognize the security and ethical risks associated with rapid, unregulated AI development but maintain that such risks can be managed through continued technological advancement. An affiliated institution of MOST, the National New Generation AI Governance Expert Committee, has issued two key policy documents: *New Generation AI Governance Principles: Developing Responsible AI* (2019) and *Ethical Norms for the New Generation of AI* (2021). These documents set out eight core principles of AI ethics: harmony, fairness, inclusiveness, privacy protection, security and controllability, responsibility, cooperation, and agile governance.[6] They also emphasize that to "predict and manage future risks" and to

[5] Gregory C. Allen, *Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security* (Center for a New American Security, 2019), https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

[6] While some of these concepts overlap with Western understandings of AI ethics—such as responsibility, fairness and inclusiveness—they carry subtly different meanings due to cultural and linguistic differences. For a detailed discussion of these interpretative differences between China and the West, see Huw Roberts et al., "Governing Artificial Intelligence in China and the European Union: Comparing Aims and Promoting Ethical Outcomes," *The Information Society* 39, no. 2 (2023): 79–97, https://doi.org/10.1080/01972243.2022.2124565.

ensure that “AI develops in a way that benefits human society”, it is essential to promote “ongoing advancements in AI technologies and research”.[7]

Technology companies have also become increasingly influential within the technology domain, particularly through their participation in consultation processes. Their growing role is evident in several instances where they have successfully shaped the content of AI regulations. For example, a comparison of the draft and final versions of the *Measures for the Management of Generative AI Services* shows that input from technology firms led to notable revisions. After consultations during the public comment period, certain restrictions on AI development were relaxed and the scope of the regulation was narrowed. Penalties for non-compliance were removed and exemptions were introduced for industry associations, enterprises, and research institutions developing or using generative AI for non-public services. The final regulation also incorporates language that directly addresses industry concerns, including commitments to “place equal emphasis on development and security” and to “promote the orderly opening of public data by type and grade, thereby expanding high-quality public training data resources”.[8] These changes demonstrate that technology companies have become increasingly influential in the technology domain and, more broadly, are contributing to shaping China’s overarching approach to AI governance.

The diplomacy domain

In the diplomacy domain, two actors play central roles: the Ministry of Foreign Affairs (MFA), which leads by virtue of its diplomatic expertise, and the MND, which has long been influential in China’s arms control diplomacy. This influence is evident in the regular involvement of MND officials in consultations during the United Nations (UN) Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS).[9] Policy think tanks are becoming increasingly active in this area as well. For instance, through Track Two diplomacy, the Centre for International Security and Strategy (CISS) has co-organized China–US and China–EU dialogues aimed at developing more operationalized proposals for the governance of AI in the military domain.[10] For these diplomatic actors, two core objectives shape their approach. The first is to protect and advance China’s geopolitical interests, particularly by achieving

[7] MOST, “New Generation AI Governance Principles – Developing Responsible AI,” 2019, https://www.most.gov.cn/kjbgz/201906/t20190617_147107.html.
[8] China Law Translate, “Comparison Chart of Current vs. Draft Rules for Generative AI,” July 13, 2023, https://www.chinalawtranslate.com/en/comparison-chart-of-current-vs-draft-rules-for-generative-ai/.
[9] Guangyu Qiao-Franco and Ingvild Bode, “Weaponised Artificial Intelligence and Chinese Practices of Human–Machine Interaction,” *The Chinese Journal of International Politics* 16, no. 1 (2023): 106–28, https://doi.org/10.1093/cjip/poac024.
[10] Qiaochu Zhang, “Navigating the In-Between Space: The Roles of Chinese Think Tanks in Artificial Intelligence Governance,” *Global Policy* 16, no. 3 (2025): 494–500, https://doi.org/10.1111/1758-5899.70053.

strategic parity with—or even gaining an advantage over—the US.[11] The second objective is to maintain a positive international image, presenting China as "committed to fulfilling its role as a responsible major country".[12]

In the context of global AI governance, these objectives translate into a dual-track stance. On the one hand, Chinese diplomatic actors argue that China should take a leading role in international initiatives on civilian AI governance to reinforce its image as a responsible global power. For example, on 26 July 2025, at the World AI Conference—which focuses primarily on AI governance in the civilian domain—the Chinese government released the Global AI Governance Action Plan, which called on all parties to take "concrete and effective actions" to advance global AI development and governance in line with the principle of promoting AI for good.[13] China has also proposed the establishment of a World Artificial Intelligence Cooperation Organization (WAICO), an initiative that implicitly frames AI governance within the civilian domain.[14] On the other hand, they maintain strategic ambiguity on military AI to safeguard China's geopolitical interests, a position particularly supported by the MND. This approach is evident in the *Global AI Governance Initiative*, which elaborates extensively on ethical principles for civilian AI—including equality, fairness, and respect for human rights—yet offers little detail on military applications. The only reference to military AI is a brief call for "a prudent and responsible attitude towards the research, development, and application of AI technologies in the military field".[15]

More specifically, China supports prohibiting only those systems it classifies as "unacceptable" components of LAWS, based on five criteria: lethality, autonomy, inability to terminate, indiscriminate killing, and self-evolution.[16] Beyond this, China remains hesitant to articulate more operational forms of regulation. For example, during UN GGE on LAWS sessions, Chinese delegations have proposed a "tiered and categorised regulation" for "acceptable autonomous weapons systems" as an alternative to the two-tiered approach favoured by other states,[17] yet they have not provided concrete guidelines for how such a system would be implemented.

---

[11] Jinghan Zeng, "The US Factor in Chinese Perceptions of Militarized Artificial Intelligence," *International Affairs* 101, no. 2 (2025): 677–689, https://doi.org/10.1093/ia/iiae323.
[12] The State Council Information Office, *A Global Community of Shared Future: China's Proposals and Actions* (2023), http://english.scio.gov.cn/node_9004328.html.
[13] Ministry of Foreign Affairs of the People's Republic of China, "Global AI Governance Action Plan," July 26, 2025, https://www.fmprc.gov.cn/mfa_eng/xw/zyxw/202507/t20250729_11679232.html.
[14] Nature Editorial, "China Is Leading the World on AI Governance: Other Countries Must Engage," *Nature* 648, no. 8093 (2025): 251–251, https://doi.org/10.1038/d41586-025-03972-y.
[15] MFA, "Global AI Governance Initiative," October 20, 2023, https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202310/t20231020_11164831.shtml.
[16] MFA, "Position Paper Submitted by China to the Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons," *Reaching Critical Will*, April 11, 2018, https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2018/gge/documents/GGE.1-WP7.pdf.
[17] MFA, "China's Position Paper on Strengthening AI Ethics Governance," November 17, 2022, https://www.mfa.gov.cn/web//ziliao_674904/zcwj_674915/202211/t20221117_10976728.shtml; MFA, "The Document Submitted by China to the UN Secretary-General on the Issue of 'Lethal Autonomous Weapon Systems'," May 23, 2024,

Table 1. Key Actors in China's Approach to AI Governance and Their Positions

Domains	Key actors	Stances on AI governance
Security	CAC and MND	China should (1) prioritize political security in AI governance, and (2) adopt different regulatory approaches for AI in the military and civilian domains.
Technology	MOST, MIIT, and technology companies	AI governance should avoid hindering the development of AI technologies, as advances in AI can themselves contribute to addressing the challenges these technologies create.
Diplomacy	MFA, MND, and think tanks	China should take the lead in global AI governance in the civilian domain while preserving strategic ambiguity regarding governing AI in the military domain.

Source: author

Recommendations

As shown in Table 1, actors across different domains hold diverse—though not necessarily conflicting—positions on AI governance. These findings have broader implications for international observers and policymakers seeking to understand China's approach and identify productive avenues for engagement in shaping global governance frameworks. Based on these insights, this contribution issues two recommendations to policymakers of other states and civil society organizations when it comes to cooperating with China on global AI governance.

1. **Policymakers and civil society actors seeking cooperation with China should focus on the civilian domain**. Across the three key domains of security, technology, and diplomacy, relevant actors in China broadly recognize the need for regulatory frameworks for civilian use of AI. Security actors view certain civilian AI applications, such as AI-generated content, as potential threats to political stability and therefore support regulatory controls. Technology actors recognize risks relating to privacy, data protection, and safety, and generally do not oppose regulation designed to mitigate these concerns. The MFA, meanwhile, sees civilian AI governance as an opportunity for China to project itself as a responsible global leader. As a result, we can expect continued—and possibly expanding—Chinese participation in international discussions on AI safety standards.[18] Engaging China on the governance of AI in the military domain, however, is significantly more difficult due to the central role of the MND.

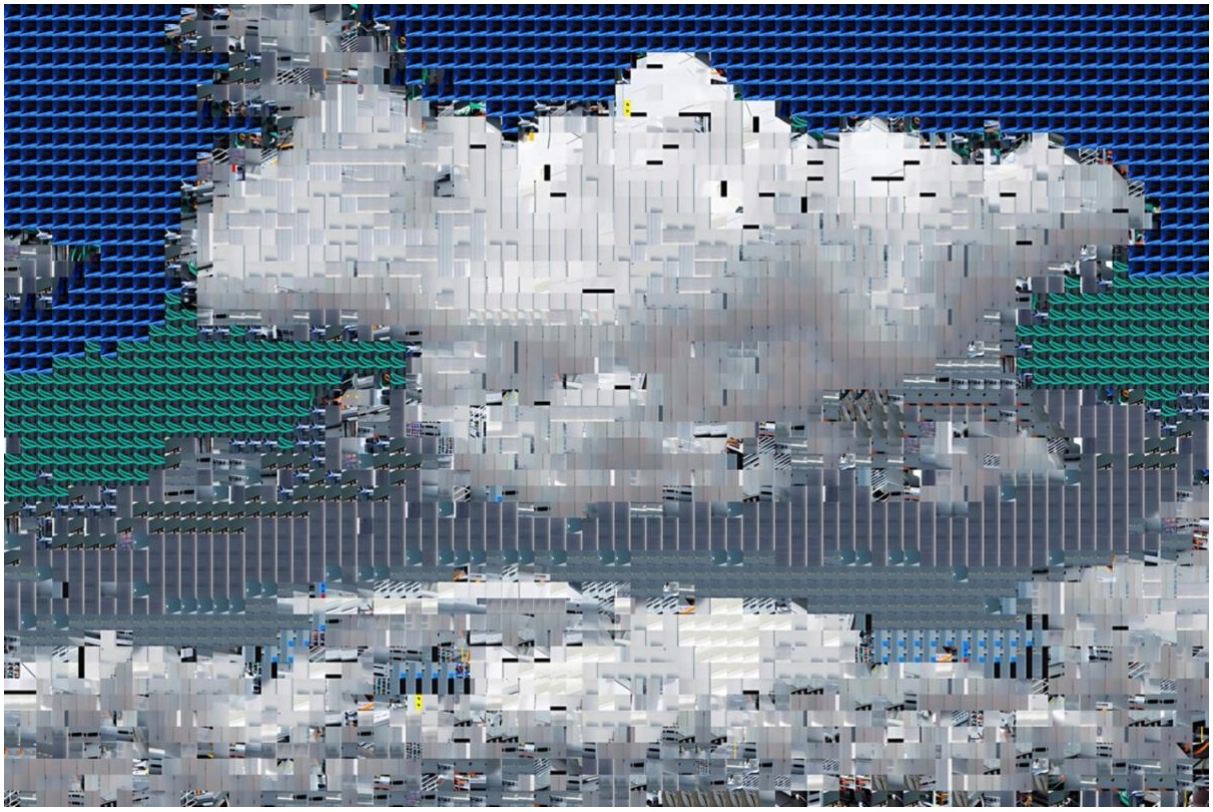
https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/fywj_674643/202405/t20240523_11310587.shtml.

[18] Guangyu Qiao-Franco and Annelotte van Beek, *China's Strategy for Global AI Governance* (Leiden Asia Centre, 2025), https://leidenasiacentre.nl/wp-content/uploads/2025/04/25-04-16-AI-report.pdf.

2. To navigate this constraint, **governments and civil society actors—based in the West or elsewhere—seeking to advance a more global framework for military AI governance through engagement with China should supplement government-to-government engagement with outreach to other relevant actors, including policy think tanks and technology companies**. Nevertheless, such actors' capacity to shape China's overall stance—particularly on the regulation of AI in the military domain—is limited by their relatively low position within the security domain of AI governance, as well as by the broader structures of China's authoritarian political system. Their roles remain subordinate to state authorities, meaning that while they contribute to the development of regulations of AI, ultimate decision-making power in the military domain rests firmly with the state.

Acknowledgements

I would like to thank Justinas Lingevičius and Anna Nadibaidze for organizing this joint policy brief and the EISA Early Career Researcher Workshop from which it emerged, as well as for their detailed and helpful comments on earlier versions of the brief. I would also like to extend my thanks to Ingvild Bode and Guangyu Qiao-Franco, whose intellectual exchanges inspired the related research that underpins this contribution. This contribution forms part of a project that has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 852123).



Nadia Piet & Archival Images of AI + AIxDESIGN / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Regulation vs. Innovation in the EU AI Policy? It Is Also About Security

Justinas Lingevicius
Vilnius University, Lithuania

Executive summary

The EU has positioned itself as an emerging leader in AI governance, framing its approach around human centrism, fundamental rights, and democracy. Building on the GDPR's precedent, the EU AI Act introduces a risk-based framework that categorizes AI applications from low to high risk, imposes prohibitions on unacceptable practices, and aims to establish a normative model for international adoption. The legislative process reflects complex institutional dynamics, with the European Commission (EC) driving expert-informed policymaking and the European Parliament (EP) injecting political debate and geopolitical considerations. However, recent initiatives, including the Apply AI Strategy and AI Continent Action Plan, demonstrate the EU's reaction to international competition, particularly from the US, prioritizing innovation, European AI products, and regulatory simplification. This shift underscores a tension between rights-driven governance and competitiveness. To address these challenges, the EU should maintain the AI Act's timeline and principles, clarify risk categories without delays, and diversify expertise in implementation bodies to ensure both effective compliance and protection of established priorities.

Introduction

The EU has positioned itself at the forefront of global AI governance, seeking not only to regulate AI within its borders but also to shape international norms through its established regulatory influence. The EU's approach to AI builds explicitly on the foundations of the GDPR, extending its logic of fundamental rights protection, market integration, and regulatory extraterritoriality into the domain of emerging technologies. This far-reaching scope highlights that EU AI policy is not merely technocratic: it is also a strategic exercise in power projection. In doing so, the EU aspires to reproduce a "Brussels effect" in AI[1]: the export of European standards globally through the gravity of its market and the normative framing of its regulatory model. As Commission President Ursula von der Leyen has emphasized, this represents the EU's ambition to advance "our own, distinctive approach to AI".[2]

[1] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020).
[2] European Commission, "Speech by President von der Leyen at the Artificial Intelligence Action Summit," February 11, 2025, https://ec.europa.eu/commission/presscorner/detail/pl/speech_25_471.

Recent initiatives such as the AI Apply Strategy and the Proposal for Regulation on simplification of AI rules indicate that, despite the adoption of the AI Act in 2024 as a landmark achievement for AI governance, the EU has been seeking to respond to international pressures, namely from the US and China, by focusing on competitiveness and even competition. However, such a market-oriented perspective overshadows the security logic inscribed in the AI Act—to safeguard individual and collective agency grounded in European values against AI and its misuse.

This contribution argues that the EU's focus on fundamental rights and democracy as being at high risk shapes the political logic and security guidelines for how the EU wants to govern AI. Attempts to move away from or delay these principles raise further questions about the renegotiation and implementation of AI governance and security logic. These tendencies are examined in two parts. First, the contribution presents key elements of EU AI policy and its security logic. Second, it discusses recent developments and potential changes in the EU's stance on the matter.

Foundations of the EU AI policy

The prioritization of AI regulation in the EU can be traced back to the beginning of Ursula von der Leyen's first Commission, where one of the strategic goals was to "ensure AI is developed in ways that respect people's rights and earn their trust".[3] The official position to consider the AI Act as part of the single market and exclude the military, despite different institutional stances on this matter, creates the impression that security is not part of the policy scope.[4]

Then, the conversation focused on the tension between regulation and innovation, presented as the ambition to "combine its technological and industrial strengths […] and a regulatory framework based on its fundamental values to become a global leader in innovation".[5] However, the AI Act adopts a security logic that is not limited to the civilian-military dichotomy but seeks to establish future-proof checks that safeguard human agency in relation to technology.

The politics of risks

The EU's AI legislation is organized around a risk-based approach, in which higher levels correspond to greater potential harm and stricter regulatory intervention. This

[3] European Commission, "Europe's Digital Decade," n.d., accessed February 6, 2025, https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade.
[4] Justinas Lingevicius, "Transformation, Insecurity, and Uncontrolled Automation: Frames of Military AI in the EU AI Strategic Discourse," *Critical Military Studies* 11, no. 2 (2025): 175–196, https://doi.org/10.1080/23337486.2024.2387890.
[5] European Commission, "White Paper on Artificial Intelligence – A European Approach to Excellence and Trust," February 19, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065.

approach distinguishes between applications with negligible risk, applications with some risk, high-risk applications, and unacceptable uses. While the EC asserts that the majority of AI systems are low-risk, high-risk systems require extensive safeguards, and unacceptable practices—such as social scoring, biometric surveillance in public spaces, or manipulation of vulnerable individuals—are prohibited.[6]

Even though they are used as a structuring policy framework, the introduced risk categories are relational and political. The definition of high risk is tied to potential impacts on fundamental rights, health, safety, and democratic processes. The Annex of the AI Act enumerates high-risk domains, including biometric identification, critical infrastructure management, education, employment, law enforcement, migration, the administration of justice, and democratic processes. However, references to AI as dangerous, harmful, or potentially injurious do not describe risk itself, but attach risk to potential harm, positioning the EU as the actor able to manage and regulate something that is not yet there. It remains to be further discussed who assesses and determines the level of potential harm, and how this is applied to the proposed risk framework.

Inscribed security logic

The emphasis on fundamental rights and their association with high risks suggests that something foundational is at risk, and the EU aims to establish oversight and accountability to ensure their protection. Here, the EU puts itself in a position of the guarantor of individual agency, focused on European values and citizens' interests. While these priorities may not be entirely new to the EU's political landscape, such a focus suggests that the EU aims to reestablish the foundational principles in the digital age, as rights are framed as endangered by AI.

A similar logic applies to a democratic political system, which is also considered at high risk. It demonstrates the collective exercise of agency linked to the EU as such, adding strategic meaning and urgency to the EU's concerns. Different documents dedicated to the AI policy indicate that AI and its uses put democratic values such as the rule of law, freedoms, rights, and democratic oversight under pressure. Therefore, the EU presents itself as a pro-democratic actor that aims to defend these values and steer future AI development in line with these principles.

In this light, the AI Act and the overall EU AI policy integrate the security logic which can be summarized as *agentic security*—to safeguard human agency, understood as the capacity to sustain human control and decision-making power across current and

[6] European Commission, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 (Artificial Intelligence Act)," June 13, 2024, http://data.europa.eu/eli/reg/2024/1689/oj/eng; European Commission, "AI Act," February 3, 2025, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

future stages of AI development.[7] However, as the policy is not explicitly considered part of security, the debate remains framed in economic terms and competitiveness. Such a tendency raises questions about the fate of these established principles and their relevance.

Is the EU reconsidering its approach?

Documents for the implementation of the AI Act, released in 2025, indicate that the EU has been reconsidering its stance. The EU appears to be increasingly influenced by international dynamics, particularly heightened competition with the US, with the new Donald Trump administration claiming ambitions to "achieve global dominance in AI".[8] In parallel, the EU also faces an internal push from major member states France and Germany to delay the implementation of AI Act.[9]

The Apply AI Strategy marks a pivot toward competitiveness, technological sovereignty, and the promotion of European AI products, signalling a recalibration of priorities that increasingly focuses on innovation. Claims such as "AI first policy where AI is considered as a potential solution" and "'buy European' approach with a focus on open-source AI solutions"[10] illustrate the change in tone where AI is not so much discussed in terms of risks and their mitigation, but promotion.

This tendency is further pursued by the EC's Proposal for Regulation on simplification for AI rules, the so-called Digital Omnibus, published in November 2025. The proposal suggests targeted simplifications and adjustments to the AI Act, including linking implementation of high-risk regulation to available standards, easing obligations for SMEs, and providing greater flexibility in post-market monitoring.[11] Even though the main argument relies on simplified rules for businesses, there is no additional detail on how the identified risks will be mitigated or how this proposal will lead to the overall delay in the AI Act's implementation.

Another initiative—the AI Continent Action Plan—further underscores the stress on competitiveness. Its key priorities rely on investing in computing infrastructure, talent, and regulatory compliance while explicitly promoting European AI products and

[7]Justinas Lingevicius, "Towards Agentic Security in the Emerging European Union AI Policy," *Contemporary Security Policy* (2026): 1–30, https://doi.org/10.1080/13523260.2025.2612518.
[8] White House, *Winning the Race. America's AI Action Plan* (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.
[9] Euronews, "France and Germany Support Simplification Push for Digital Rules as Commission preps AI Act review," November 18, 2025, https://www.euronews.com/my-europe/2025/11/18/france-germany-support-simplification-push-for-digital-rules-as-commission-preps-revision-.
[10] European Commission, "Apply AI Strategy," n.d., accessed November 9, 2025, https://digital-strategy.ec.europa.eu/en/policies/apply-ai.
[11] European Commission, "Digital Omnibus on AI Regulation Proposal," November 19, 2025, https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal.

innovation to “ultimately become a leading AI Continent”.[12] The ambition to have international influence remains, but it is more focused on infrastructure investment and accelerating AI adoption than on rules and standards. Such a tendency reflects a growing emphasis on competition, intersecting with pressures to accelerate *European* AI development and to pursue power dynamics on the global stage. If this direction becomes prioritized, it remains unclear whether key elements of agentic security will also be reconsidered.

Recommendations

The EU’s AI policy aims not only to establish a distinctive European AI governance but also to inscribe a security logic focused on safeguarding both individual and collective agency against AI and its misuses. However, the EU’s recent adjustments—driven by international competition and pressures to accelerate innovation—highlight ongoing struggles to balance normative principles with industrial objectives. The following recommendations suggest that the EU should align its AI governance implementation without delay and clarify the remaining ambiguities to make the process more accountable and inclusive. Therefore, EU policymakers should:

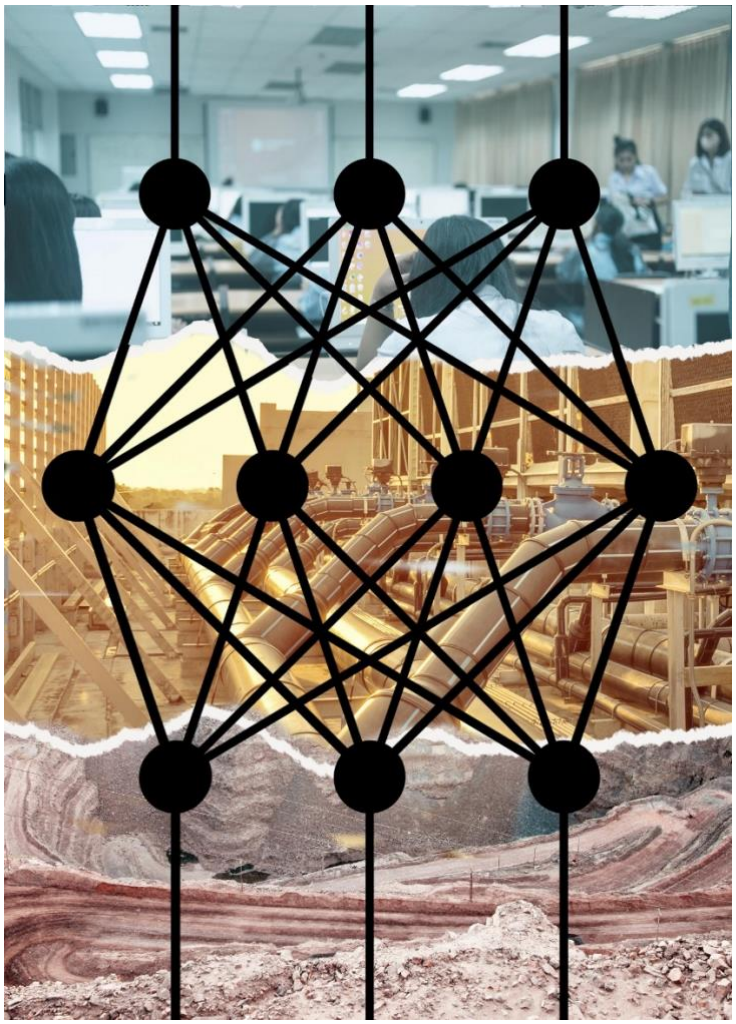
1. **Maintain the AI Act’s timeline and core principles.** The EU should uphold the original implementation schedule and adhere to the main principles agreed in the AI Act. It is important to assess their application and implementation not only to demonstrate compliance but also to create certainty for businesses and related stakeholders. Further delay would even increase uncertainty and raise questions about the relevance of the rules in the context of constant technological change. Preserving the integrity of the rights-driven framework reinforces the EU’s credibility as a global standard-setter and influences further discussions on AI governance and its priorities.

2. **Explicitly endorse security in the AI policy.** The EU should move away from this regulation-versus-innovation dichotomy by explicitly incorporating the security elements into its AI policy. This point could be addressed by clarifying and explaining how potential AI-related harm to fundamental rights and democracy will be measured at both the national and EU levels. The security argument would also enable the EU to argue the relevance of established rules, as international AI governance remains fragmented.

3. **Diversify expertise in implementation and oversight bodies.** Current initiatives to involve external expertise, such as the EC’s proposed scientific panel, prioritize technical expertise while largely excluding legal, ethical, and

[12] European Commission “The AI Continent Action Plan,” April 9, 2025, https://digital-strategy.ec.europa.eu/en/library/ai-continent-action-plan.

human rights perspectives.[13] To adequately assess the societal and political implications of AI use, the EU should ensure that implementation and advisory bodies include a balanced mix of engineers, legal experts, ethicists, and human rights specialists. Diverse and inclusive expertise would strengthen the capacity and better prepare to protect fundamental rights and democratic cohesion while assessing and deciding on potential harm.



Kathryn Conrad & Rose Willis / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

[13] European Commission, “Commission Seeks Experts for AI Scientific Panel,” June 16, 2025, https://digital-strategy.ec.europa.eu/en/news/commission-seeks-experts-ai-scientific-panel.

Digital Colonialism in Global AI Governance: Addressing Power Imbalances and Protecting Indigenous Self-Determination

Elena Kavanagh
University of Cambridge, UK

Executive summary

Digital colonialism refers to the reproduction of colonial patterns of domination through digital technologies, data infrastructures, and AI. This contribution examines how digital colonialism is reflected in the emerging governance of AI, why it threatens global equity and cultural resilience, and why it is a significant concern for AI safety. Indigenous communities have particular risks when their land-based knowledge and cultural expressions are digitized and integrated as data into AI systems without Free, Prior and Informed Consent (FPIC). The contribution argues that addressing digital colonialism requires governance frameworks deriving from Indigenous peoples' right to self-determination, as exemplified by inclusive governance in the context of the Arctic. The contribution recommends that states, international institutions, corporations and civil society adopt and strengthen meaningful mechanisms of participation that bring together different knowledge systems and multiple ways of knowing into global AI governance.

Introduction

Digital colonialism reflects structural imbalances in who controls digital infrastructure, who owns and extracts the data used to train AI systems, who meaningfully shapes global technical standards, and whose knowledge systems are recognized as legitimate in AI development.[1] Dominated by major powers, AI ecosystems are shaped by the political, economic, and cultural priorities of their respective states of origin. These technologies, exported globally, can embed external values and governance logics that may not align with local, Indigenous, or Global South contexts.[2]

[1] Aníbal Quijano and Michael Ennis, "Coloniality of Power, Eurocentrism, and Latin America," *Nepantla: Views from South* 1, no. 3 (2000): 533–580, https://muse.jhu.edu/article/23906.
[2] Arthur Gwagwa, "Resisting Colonialism – Why AI Systems Must Embed the Values of the Historically Oppressed," in Alex Krasodomski (ed.), *Artificial Intelligence at the Challenge for Global Governance* (Chatham House, 2024), https://www.chathamhouse.org/2024/06/artificial-intelligence-and-challenge-global-governance/06-resisting-colonialism-why-ai.

Meaningful participation remains heavily weighted toward a small cluster of technologically advanced actors. The asymmetry concentrates decision-making power and causes data extraction practices. It also embeds Western epistemologies, or ways of knowing and understanding the world, into global technical standards. The integration of digital systems into everyday life risks reproducing colonial patterns of dispossession and control, particularly for Indigenous peoples.

This contribution examines digital colonialism as a governance challenge, highlights its implications for human rights, and identifies policy pathways to mitigate its impacts. It emphasizes the importance of inclusive and pluralistic AI governance frameworks that prioritize Indigenous participation and knowledge sovereignty. The primary legal foundation for this analysis is the adherence to Indigenous peoples' right to self-determination.[3]

While this contribution centres primarily on the impacts of digital colonialism on Indigenous communities and their rights to self-determination, it also recognizes that many of the structural dynamics discussed, including power asymmetries, data extractivism, and exclusion from governance processes, are shared by Global South states and other marginalized actors within global AI governance.

Understanding digital colonialism in the AI era

The global expansion of AI is generating profound geopolitical, social, and cultural consequences, as AI systems increasingly influence decisions across all spheres of governance.[4] Despite this growing impact, the benefits and burdens of AI are distributed unevenly.[5] Countries with advanced technological infrastructure continue to dominate AI model design. In 2024, global corporate investment in AI reached a record of $252.3 billion, with private investment climbing sharply, reflecting the rapid acceleration of AI development worldwide and the concentration of capital among a small number of technologically advanced economies and corporations.[6]

Power asymmetries in emerging global AI governance mirror long-standing patterns in extractive industries and international relations. At the same time, AI governance introduces new risks by expanding data extraction, automating cross-border decision-making, and embedding technical standards that can lock these inequalities into global

[3] United Nations, *United Nations Declaration on the Rights of Indigenous Peoples*, General Assembly Res. 61/295, adopted September 13, 2007, arts. 3 and 18, https://www.un.org/development/desa/Indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf.
[4] Huw Roberts et al., "Global AI Governance: Barriers and Pathways Forward," *International Affairs* 100, no.3 (2025): 1275–1286, https://doi.org/10.1093/ia/iiae073.
[5] United Nations General Assembly, "Resolution Adopted by the General Assembly on 21 March 2024: Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development (A/RES/78/265)," April 1, 2024, https://docs.un.org/en/A/res/78/265.
[6] Nestor Maslej et al., The *AI Index Report 2025* (Stanford University, 2025), https://doi.org/10.48550/arXiv.2504.07139.

digital infrastructure. The governance frameworks that regulate AI, and the global markets in which they operate, reinforce existing power asymmetries between the Global North and South;[7] and between the former colonizers and the colonized.[8] As a result, global AI governance risks constitute a high-stakes decision-making arena in which excluding non-Western epistemologies, including Indigenous perspectives and ways of knowing, leads to systematically skewed and distorted policy outcomes.

Digital colonialism describes this emerging system of power. At the same time, it manifests through overlapping political and economic mechanisms. These dynamics are exacerbated by unequal access to technological capabilities, persistent geopolitical asymmetries, and the global concentration of data infrastructures. As it reshapes power relations and undermines the principles of equitable governance, digital colonialism has significant consequences for global decision-making and human rights.

Concentration of rule-making power

Most international AI standards, safety guidelines, and regulatory initiatives originate from a handful of states and corporations in Europe, North America, and East Asia. This concentration is evident in major AI governance events of recent years, in which lower-income countries and Indigenous peoples remain underrepresented. Asymmetry gives disproportionate influence on actors who shape global norms according to their own priorities. This imbalance overlooks the value of understanding local contexts, which is essential for creating AI frameworks and governance models that are equitable and context sensitive.

A governance system dominated by a narrow set of actors lacks global legitimacy. The exclusion of most of the world's population reduces trust and weakens the effectiveness of international agreements. Without structural reforms, new AI governance bodies risk reproducing the inequalities that have long affected multilateral decision-making.

Data extractivism and ownership

Vulnerable to "data poisoning", AI systems rely on massive datasets, many of which are scraped indiscriminately from the public sphere.[9] This process often includes cultural materials, images, languages, and knowledge systems belonging to

[7] In this context, the 'Global North' generally refers to wealthier, industrialized countries with a history of economic and political dominance, while the 'Global South' refers to lower-income and developing regions that have experienced colonial exploitation.

[8] Gordon LaForge, Robert Muggah, and Gabriella Seiler, *Bridging the AI Governance Divide*, Policy Brief 120 (Igarapé Institute & New America, 2024), https://www.t20brasil.org/media/documentos/arquivos/TF05_ST_05_Bridging_the_AI_gov66cdcbf06f991.pdf.

[9] Vasilios Mavroudis and Chris Hicks, "LLMs May Be More Vulnerable to Data Poisoning Than We Thought," *The Alan Turing Institute*, October 9, 2025, https://www.turing.ac.uk/blog/llms-may-be-more-vulnerable-data-poisoning-we-thought.

communities that neither consented to their use nor benefited from the outcomes. For Indigenous peoples, the extraction of traditional knowledge into AI training sets continues long-standing colonial patterns of appropriation.[10] Without clear data governance and intellectual property rights, communities risk losing authority over how their identities, languages, and cultural expressions are used or represented.

Epistemic domination and cultural erasure

AI systems often reflect a narrow set of worldviews. Large language models, for instance, tend to privilege Western scientific and cultural narratives, which can erase or distort perspectives from the Global South and Indigenous communities.[11] Researchers have noted that culturally grounded forms of knowledge, particularly those rooted in relationality and land-based practices, are difficult to capture in data formats designed around Western epistemologies.[12] As these systems become embedded in global governance, they risk codifying epistemic hierarchies into digital infrastructures.

For Indigenous peoples, digital colonialism threatens cultural continuity, understood as the ability of communities to sustain, transmit, and adapt their culture across generations. This directly undermines the communities' right to self-determination and to govern their cultural, social, and political futures.

Infrastructural dependence and impacts

Physical infrastructures, such as the data centres that sustain AI, are increasingly sited in regions with available land, water, and energy resources, including areas inhabited by Indigenous and rural communities, and are primarily owned by multinational corporations.[13] For example, in central Mexico's Querétaro state, a boom in data centre construction has allowed facilities to bypass environmental reporting requirements, leading residents to raise concerns about the effects on water supplies

[10] Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press, 2019).
[11] Rida Qadri et al., "Risks of Cultural Erasure in Large Language Models," *arXiv* (January 2, 2025), https://arxiv.org/abs/2501.01056.
[12] Reen-Cheng Wang, Ming-Che Hsieh, and Liang-Chun Lai, "From Tacit Knowledge Distillation to AI-Enabled Culture Revitalization: Modeling Knowledge Cycles in Indigenous Cultural Systems," *Social Sciences* 15, no. 7 (2026): 1–21, https://doi.org/10.3390/socsci15010007.
[13] Ben Craske, "Indigenous-Led Data Centre Planned for Alberta Power Plant," *Data Centre Magazine*, July 16, 2025, https://datacentremagazine.com/news/indigenous-led-data-centre-planned-for-alberta-power-plant; Indigenous Energy Monitor, "Indigenous Participation in Canada's Emerging Data Centre Landscape," June 28, 2025, https://www.indigenousenergymonitor.ca/post/indigenous-participation-in-canada-s-emerging-data-centre-landscape; Ka'ulawena Alipio et al., "Indigenous Data Sovereignty, Circular Systems, and Solarpunk Solutions for a Sustainable Future", *Proceedings of the Pacific Symposium on Biocomputing 2025* (Stanford University, 2025), https://psb.stanford.edu/psb-online/proceedings/psb25/alipio.pdf; Honor the Earth, "Proposed Data Centers in Indian Country," October 17, 2025, https://storymaps.arcgis.com/stories/724e9dc3b9f64cb1a9c219b9d02eaad4.

and ecosystem health in an already water-stressed region.[14] Data centres in Chile and Mexico have significantly increased local water and energy demand in regions already affected by scarcity.[15]

AI-driven economic systems depend on access to data and compute power. States or corporations that control these resources hold significant economic advantages, potentially deepening global inequalities. Without policies that regulate data exploitation and ensure fair distribution of benefits, digital colonialism will continue to shape global economic hierarchies.

The value of the pluralistic model for AI governance

While no global AI governance institution has yet been established, a growing set of international initiatives and coordination mechanisms is shaping emerging norms and regulatory approaches. Within this context, certain international governance models offer useful institutional lessons.[16] One of the most relevant is the Arctic Council, which embeds Indigenous peoples as permanent participants with formal procedural rights. This structure ensures that Indigenous organizations directly influence environmental, scientific and political decisions affecting their territories and communities.[17]

While the Arctic Council operates in a geographically specific context, its institutional design offers transferable lessons for AI governance. Its permanent participant model could be adapted to emerging AI governance forums by granting Indigenous organizations formal decision-making status rather than limiting participation to observer or consultative roles. In practice, this could take the form of reserved seats for Indigenous representatives within multilateral AI governance bodies, co-governance arrangements for issues affecting Indigenous data and territories, and procedural rights to review or contest policies that directly impact Indigenous communities.

The Arctic Council demonstrates that it is both possible and beneficial to institutionalize Indigenous knowledge and participation within an intergovernmental structure.[18]

---

[14] Pablo Medina Uribe et al., “Many Latin Americans Living Near Data Centers Don’t Feel Welcome in the Future,” *Tech Policy Press*, September 12, 2025, https://www.techpolicy.press/many-latin-americans-living-near-data-centers-do-not-feel-welcome-in-the-future/.

[15] Diana Baptista, “As AI Fuels Growth of Data Centres, Critics Fight Back,” *Context,* June 9, 2025, https://www.context.news/ai/as-ai-fuels-growth-of-data-centres-critics-fight-back; Claudia Urquieta and Daniela Dib, “U.S Tech Giants are Building Dozens of Data Centers in Chile. Locals are Fighting Back,” *Rest of World*, May 31, 2024, https://restofworld.org/2024/data-centers-environmental-issues/; Pablo Jiménez Arandia, “How We Investigated the Backyard of AI in Spain, Chile and Mexico,” *Pulitzer Center*, September 25, 2025, https://pulitzercenter.org/resource/how-we-investigated-backyard-ai-spain-chile-and-mexico.

[16] Timo Koivurova, “The Arctic Council: A Testing Ground for New International Environmental Governance,” *Brown Journal of World Affairs* 19, no. 1 (2012), 131–144, https://www.jstor.org/stable/24590933.

[17] Elena Kavanagh, “Arctic Governance: An Analysis of a Treaty-Based Cooperation Hypothesis,” *Spanish Yearbook of International Law* 27 (2023): 257–265, https://doi.org/10.36151/SYBIL.2024.013.

[18] Dorothée Cambou, “Enhancing the Participation of Indigenous Peoples at the Intergovernmental Level to Strengthen Self-Determination: Lessons from the Arctic,” *Nordic Journal of International Law* 87, no. 1 (2018): 26–55, https://doi.org/10.1163/15718107-08701002.

Applying lessons from the Arctic Council to global AI governance suggests that meaningful structural participation should be a core component of any legitimate international AI framework.

Towards a decolonial AI governance framework

Addressing digital colonialism requires structural changes in how emerging global AI governance frameworks are being developed and coordinated, rather than assuming a fully established system already exists. These changes must ensure equal participation and integrate multiple ways of knowing into regulatory frameworks.

Meaningful participation

Pluralistic governance demands mechanisms that allow Global South states and Indigenous peoples to contribute to standard-setting. This approach differs significantly from the Inclusive AI Governance discourse, which has been largely proposed by institutions in the Global North.[19] Based on the right to self-determination, participation must extend beyond consultations and instead provide decision-making influence over processes affecting their rights and interests.

For example, multilateral AI initiatives could establish permanent seats for Indigenous and Global South representatives on international standard-setting bodies (similar to the permanent participant model of the Arctic Council), create co-governance committees jointly chaired by state and Indigenous delegates to oversee AI ethics and deployment protocols, and embed procedural rights for review or veto of decisions that impact Indigenous data, cultural expressions, or territorial uses. Institutional reforms may include guaranteed seats for Indigenous organizations in AI governance bodies, co-governance arrangements, and rights to review or veto decisions that affect their territories or knowledge systems.

Data sovereignty and consent

The right to govern one's knowledge and data must be recognized as a foundational element of AI governance. Indigenous data sovereignty frameworks, including the CARE Principles[20] and the principle of FPIC, offer concrete pathways to ensure respectful and equitable data practices. Embedding these principles into national legislation and global AI agreements would prevent exploitative data extraction and create accountability mechanisms for technology developers.

[19] Marie-Therese Png, "The Critical Roles of Global South Stakeholders in AI Governance," in Justin B. Bullock, et al. (eds.), *The Oxford Handbook of AI Governance* (Oxford University Press, 2022), 981–1014.
[20] Stephanie Russo Carroll et al., "The CARE Principles for Indigenous Data Governance," *Data Science Journal* 19, no. 1 (2020): 43, https://doi.org/10.5334/dsj-2020-043.

Capacity and resource equity

Equitable participation in global AI governance requires investment in local research capacity, infrastructure, and education. Many communities cannot meaningfully participate without targeted support. A global AI capacity fund, housed within an existing multilateral institution, such as UNESCO, the UN Development Programme (UNDP), or the International Telecommunication Union (ITU), could help provide financial assistance, technical training, and infrastructure resources to underserved regions.

Conclusion

Digital colonialism is one of the biggest governance challenges of the AI era. The exclusion and marginalization of Indigenous and other communities lead to systematically distorted decisions. A decolonial and pluralistic approach to AI governance requires meaningful participation, legal recognition of data sovereignty, integration of diverse epistemologies, and equitable distribution of technological resources. This contribution has argued that the principles of self-determination discussed in current Indigenous governance discourse and the example of institutions such as the Arctic Council demonstrate that inclusive governance is both possible and necessary.

Recommendations

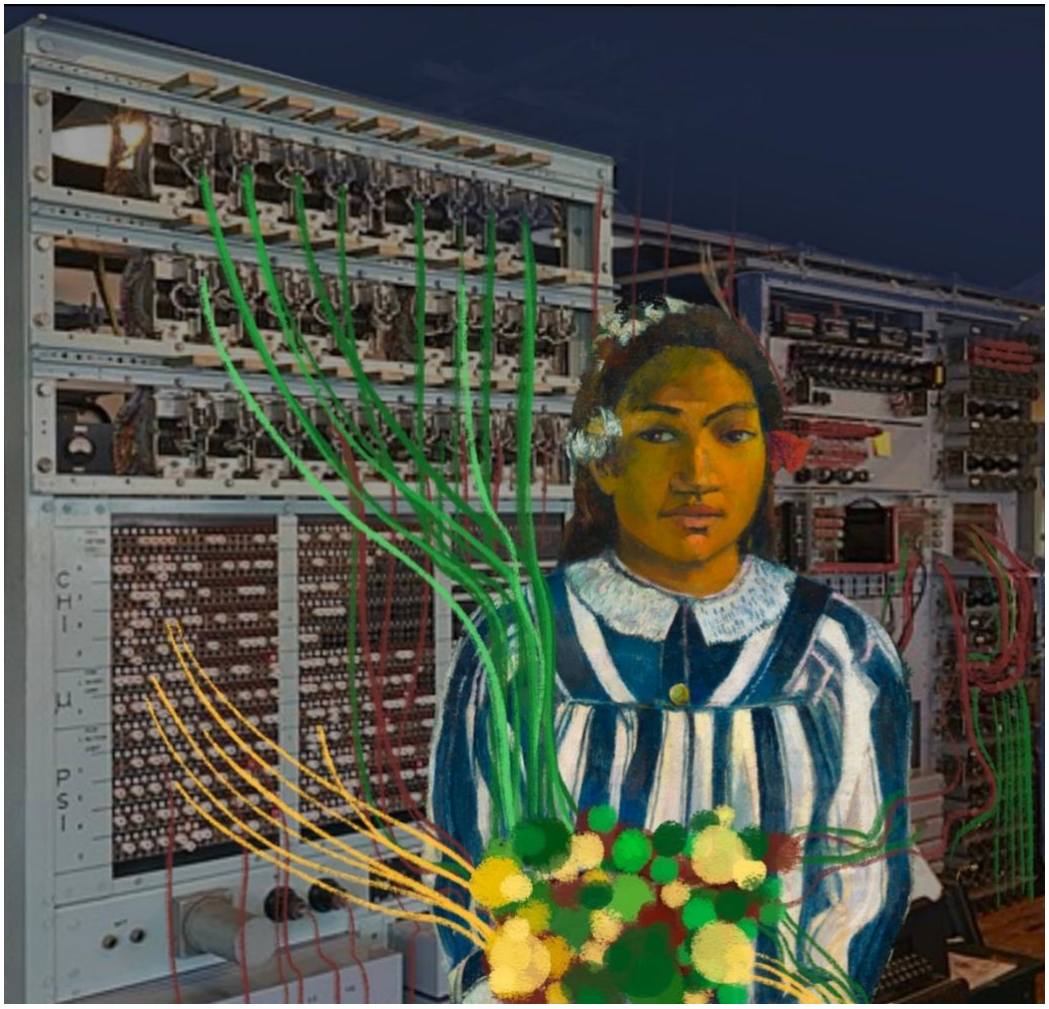
Based on the global dynamics of digital colonialism, this contribution issues the following policy recommendations:

1. **States should recognize Indigenous data sovereignty** in national law and implement consent-based data governance frameworks that require explicit authorization for the collection, use, and sharing of community data in order to prevent extractive practices.

2. **International institutions should embed pluralism in AI governance design.** Reform emerging AI governance frameworks by institutionalizing pluralistic participation models, including permanent Indigenous representation, procedural rights in decision-making processes, and mechanisms to integrate Indigenous knowledge systems into global AI standards. Moreover, the international FPIC standards specific to AI should be established, making consent a prerequisite for data extraction, model training, and digital projects affecting Indigenous communities.

3. **Corporations should adopt Indigenous data governance frameworks**, integrate Indigenous advisory bodies with real decision-making authority, and commit to transparent, culturally respectful AI data practices.

4. **Civil society should monitor AI impacts and support accountability.** This means conducting independent audits of AI systems, raising awareness about digital colonialism, and supporting Indigenous-led research and advocacy initiatives that promote community rights and accountability.



Hanna Barakat & Cambridge Diversity Fund / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Technology for Who? Artificial Intelligence at the Threshold of Civil-Military Relations

Benjamin T. Johnson
University of Groningen, Netherlands

Executive summary

The advent of AI and its centrality to economic and geopolitical competition, as well as its role in transforming the civil and military sectors, creates regulatory and governance tensions that require consideration. While the distinction between the civil and military domains is conceptually straightforward, it is difficult to trace in practice. The EU AI Act (the Act) represents the most ambitious global effort to establish governance norms and rules for the development and use of AI. However, the AI Act's exclusion of AI developed and or used for military and national security purposes reflects these regulatory tensions. The EU's focus on investing in 'dual-use' technologies rhetorically bridges the civil-military divide. This contribution argues that the EU's 'dual-use' focus is ill-defined, particularly regarding how to identify when a technology is developed or used in defence and national security interests rather than for civilian applications. As the EU and Member States push for greater social-military mobilization in preparation for general war, the risk is that AI will be increasingly militarized to avoid the AI Act's regulatory power. To address this risk, European policymakers should work to define dual-use technologies beyond vague notions of civilian and military use and operationalize them concretely.

Introduction

The advent of AI as a general-purpose suite of technologies represents one of the most significant social, political, and economic developments of our time. AI's transformative potential is especially recognized in the military domain, with militaries endeavouring to accelerate AI development and adoption across everything from strategic planning and intelligence to decision-making and autonomous weapons systems.[1]

[1] Toni Erskine and Steven E. Miller, "AI and the Decision to Go to War: Future Risks and Opportunities," *Australian Journal of International Affairs* 78, no. 2 (2024): 135–47, https://doi.org/10.1080/10357718.2024.2349598; Michele A. Flournoy, "AI Is Already at War: How Artificial Intelligence Will Transform the Military," *Foreign Affairs*, October 24, 2023, https://www.foreignaffairs.com/united-states/ai-already-war-flournoy; Adib Bin Rashid et al., "Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges," *International Journal of Intelligent Systems* 2023, no. 1 (2023), https://doi.org/10.1155/2023/8676366.

Governments around the world are accelerating regulatory and governance efforts to benefit from AI's economic potential while minimizing social harms.[2] The AI Act is the most ambitious global regulatory and governance effort on AI, providing a comprehensive framework for developing and using AI systems in the civilian realm. The AI Act is framed with a lens of protecting European values and safety while enhancing the common market. Importantly, the AI Act does not apply to AI systems developed and used 'exclusively' for military, defence, and national security purposes.

At the same time that the EU is attempting to establish governance norms and standards, there is a push for more investment and diversified investment vehicles in military and defence, particularly for technology research and development.[3] Much of this investment is promoted through the language of 'dual-use' technologies; that is, technology with both civilian and military applications.[4]

While the Act would apply to dual-use AI systems used in a civilian domain, it lacks an explicit definition of 'dual-use'. This contribution highlights the risks of not defining 'dual-use' and recommends that EU and Member States officials operationalize this concept. While defining and operationalizing 'dual-use' in concrete terms is not a guarantee that the AI Act will retain its regulatory power, it is a critical step if the EU wishes to diminish the risk of broadly militarizing AI development and use.

What is 'dual-use' technology?

The emphasis on dual-use to frame AI and other technologies (such as drones) strategically neutralizes political and economic discourse about them. Dual-use, in this sense, is a rhetorical device and conceptual shorthand used to legitimize greater investment in technology and infrastructure with wider social applications beyond purely military and defence needs while simultaneously side-stepping greater public scrutiny. This manoeuvre rests on a classic binary distinction between the civilian and military arenas, replicated in the AI Act's legal framework. The AI Act's legal framework does not explicitly discuss or define dual-use technology.

---

[2] Arjun Ghosh et al., "Artificial Intelligence in Governance: Recent Trends, Risks, Challenges, Innovative Frameworks and Future Directions," *AI & SOCIETY* 40, no. 7 (2025): 5685–707, https://doi.org/10.1007/s00146-025-02312-y.

[3] European Commission, "EU Defence Industry Transformation Roadmap: Unleashing Disruptive Innovation for Defence Readiness," November 19, 2025, https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en?filename=EU-Defence-Industry-Transformation-Roadmap.pdf; European Commission, "From AI to Quantum: How the European Defence Fund Shapes the Future of EU Defence Technologies," December 15, 2025, https://defence-industry-space.ec.europa.eu/ai-quantum-how-european-defence-fund-shapes-future-eu-defence-technologies-2025-12-15_en.

[4] European Commission, "Dual-Use Technologies," 2025, https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/dual-use-technologies_en; Bruno Oliveira Martins and Neven Ahmad, "The Security Politics of Innovation: Dual-Use Technology in the EU's Security Research Programme," in Antonio Calcara, Raluca Csernatoni, and Chantal Lavallée (eds.), *Emerging Security Technologies and EU Governance* (Routledge, 2020).

Instead, it distinguishes between the civilian and military sectors in broad terms, with the Act's regulatory authority applying only to the former. The AI Act's core balancing manoeuvre is to advance EU normative values and economic interests without hindering military innovation and defence, which is beyond the EU's legal capacity, as national security is strictly the domain of Member States. However, the AI Act's explicit concern for the civilian realm and its exclusion of the military dimension represents an inconsistency relative to the EU's wider military efforts, because evidence indicates that the Act itself integrates military thinking within its framework.[5]

While the civil-military binary may appear unproblematic conceptually and legally, it is difficult to maintain in practice. This problem is especially apparent as the Big Tech AI developers—Google, Microsoft, Amazon, and others—increasingly straddle military and civilian spaces.[6] The EU's federalist architecture especially complicates these efforts. Member States have the final say on their national security matters and are likely to push back against any infringement on their sovereignty, as France has already done with the Act.[7]

These issues create regulatory tensions and pressures that the EU AI Act does not readily address. More importantly, the Act's explicit regulatory distinction between AI use in civilian and military systems could incentivize developers to frame or shift projects toward military, defence, and national security applications to avoid the Act's regulation.

Blurring domains

The EU AI Act is currently in a phased implementation period, having entered into force on August 1, 2024. Key provisions have already become active, with the majority of the rules, including those for high-risk systems, set to apply in August 2026, and full applicability scheduled for August 2027. According to the Act's wording, its core purpose is

> to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter,

[5] Justinas Lingevicius, "Transformation, Insecurity, and the Uncontrolled Automation: Frames of Military AI in the EU AI Strategic Discourse," *Critical Military Studies* 11, no. 2: 175–196 (2025), https://doi.org/10.1080/23337486.2024.2387890

[6] Lucas Maaser and Stephanie Verlaan, *Big Tech Goes to War: Uncovering the Growing Role of US and European Technology Firms in the Military-Industrial Complex* (Studien, 2022), https://www.rosalux.de/fileadmin/rls_uploads/pdfs/Studien/Studien_5-22_BigTech_en_web.pdf; Anthony King, *AI, Automation, and War: The Rise of a Military-Tech Complex* (Princeton University Press, 2025).

[7] Maria Maggiore, Leïla Miñano, and Harald Schumann, "France Spearheads Member State Campaign to Dilute European AI Regulation," *Investigate Europe*, January 22, 2025, https://www.investigate-europe.eu/posts/france-spearheads-member-state-campaign-dilute-european-artificial-intelligence-regulation.

> including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation.[8]

The notions of 'human-centric' and 'trustworthy' AI are not explicitly defined but rather serve as normative guiding principles that are translated into more precise obligations governing the development and use of AI. How does the Act treat defence and military technologies? Article 2.3 of the Act states:

> This Regulation does not apply to AI systems where and in so far they are placed on the market, put into service, or used with or without modification exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.
>
> This Regulation does not apply to AI systems which are not placed on the market or put into service in the Union, where the output is used in the Union exclusively for military, defence or national security purposes, regardless of the type of entity carrying out those activities.[9]

These stipulations are important because they exempt any AI system or the outputs of that system that are developed and used 'exclusively' for military and national defence purposes from the Act's regulatory and oversight power. While the Act adopts a risk-based framework that imposes different obligations (such as for police agencies), its exemption for military, defence, and national security purposes creates a boundary that can be strategically exploited or inadvertently blurred.

From securitization to militarization

Distinguishing between the military and civilian arenas of political and social activity is appealing but fundamentally flawed, as it is premised on a narrow institutional view of militaries and the contemporary nature of security, while misrepresenting the nature of technology, especially AI.

Both the AI Act and the idea of 'dual-use' are premised on a clean separation between civilian and military spheres. However, as seen in earlier security paradigms such as the War on Terror, security logics and efforts can gradually extend into the domains of civilian governance (securitization). While the Act's risk framework regulates dual-use technology through its use and effects, it does not formally regulate its transfer or provide special consideration for developers that operate across the civil-military and national security domains.

[8] European Commission, "AI Act Explorer- Chapter 1: General Provisions - Article 2: Scope," 2026, https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-2.
[9] Ibid.

Recent efforts among Member States and at the EU level to push for rearmament, investment, and society-wide readiness for the real possibility of a large-scale interstate war have already sown the seeds of militarization across civilian life, such as education.[10] By militarization, I am referring to the growing influence of military goals, logics, and values across society and the economy. Maintaining the civilian/military distinction in practice is far more difficult than is appreciated.

Importantly, this formal distinction in the Act potentially incentivizes developers, users, and policymakers to increasingly rely on framing AI within a defence and national security lens to avoid the Act's regulatory power, reducing oversight and transparency. Big Tech AI actors are especially keen on reducing regulation and regulatory 'red tape' to fuel innovation. While the Act aims to improve accountability, it may encourage the opposite as civilian/military boundaries are blurred. The EU's *Readiness 2030* plan addresses the issue directly, stating that

> A handful of critical and foundational technologies like AI, quantum, biotech, robotics, and hypersonic are key inputs for both long-term economic growth and military pre-eminence. Boosting innovation is key for this. As such, technology diffusion for commercial purposes must be reconciled with more rigid technology ecosystems to advance national security objectives.[11]

'Dual-use' is the policy key to reconciling these tensions. *Readiness 2030* states that "[s]trengthening the logistics of the armed forces also matches the need to make our economy more connected and competitive—a perfect fit in terms of dual use".[12]

Investment through venture capital and private equity funds is being directed through the European Investment Fund's (EIF) Defence Equity Facility, which supports "[investment] in European companies innovating defence technologies with dual use potential".[13] Similar to the AI Act, *Readiness 2030* and the EU's *Technology Roadmap* frame AI systems as something that can be regulated by simply moving them in and out of different use cases.

Just as the War on Terror increasingly securitized many aspects of our lives and legitimated the increasing reach of the surveillance state, current European defence rhetoric and policy efforts, along with the dominance of geopolitical competition as a framing mechanism, implicate the real and likely possibility of increased militarization.

[10] "Dear University, We Need to Talk About Militarization," *Univers: The Independent News Source of Tilburg University*, December 4, 2024, https://universonline.nl/nieuws/2024/12/04/dear-university-we-need-to-talk-about-militarization/.
[11] European Commission, *White Paper for European Defence – Readiness 2030* (2025): 5, https://defence-industry-space.ec.europa.eu/eu-defence-industry/white-paper-european-defence-readiness-2030_en.
[12] Ibid., 8.
[13] European Investment Fund, "Defence Equity Facility," n.d., accessed February 1, 2026, https://www.eif.org/flagship-initiatives/investeu/defence-equity-facility.

This trend is especially evident as AI regulatory standards at the national level appear to be increasingly caught in a "race-to-the-bottom" environment.[14] As militarization creeps in, the incentive is to make everything national defence and security-related, particularly in the name of innovation.

The risks of not defining 'dual-use'

Several concerns emerge from the blurring of the civil-military lines in European AI governance. The AI Act regulates AI primarily as a market product with defined purposes. However, the Act is not necessarily well-suited for governing AI systems that migrate across civilian and security contexts. This is problematic because AI systems are fundamentally conditioned through key decisions at the outset, including what data is used for training, what the system's objectives are, what errors are tolerated, and others. These issues lead to AI's 'black box' problem, where AI outputs are obscured by opaque processes that hinder transparency and desirable goals, such as trust and fairness.

Regulating AI by classifying its use does not necessarily solve many of the problems associated with 'black box' opaqueness. Fundamentally, the logic driving investment in AI innovation and deployment through EU Readiness efforts is at odds with EU regulatory efforts.

Although 'dual-use' is currently used loosely, its growing centrality in EU defence and innovation policy makes the need for more explicit criteria clear. This issue is not limited to the AI Act but reflects a wider issue across the EU's digital agenda and the tendency to deploy 'dual-use' as a catch-all term that aligns industrial competitiveness within the common market with the demand for technological innovation in the military sphere. Such a tendency demonstrates avoidance of the inherent tensions between militarization and EU norms and values.

If we are to protect the AI Act's core normative goals along with EU citizens from AI's riskiest applications, we need to operationalize 'dual-use' in concrete terms and metrics. It means clearly identifying when an AI system is 'civilian' and when it is 'military' and related to national defence and security—from inception, to research and development, design, and use.

Recommendations

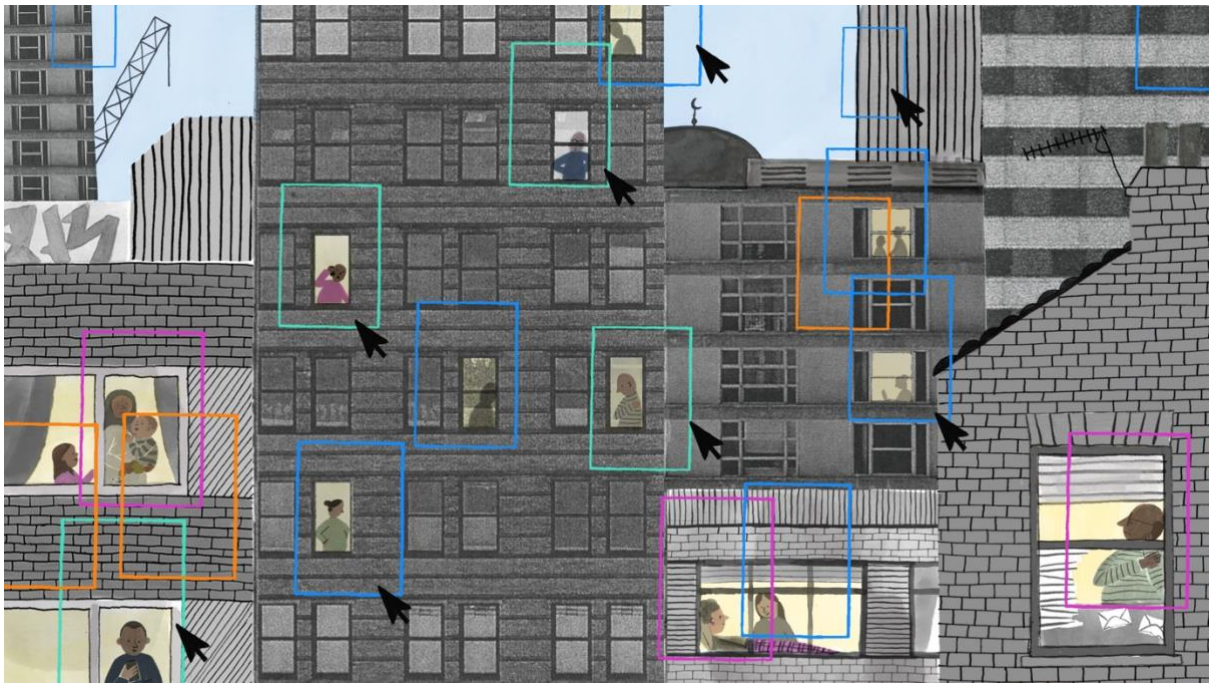
This contribution issues the following recommendations to EU officials and Member States policymakers:

[14] Nicholas Emery-Xu, Richard Jordan, and Robert Trager, "International Governance of Advancing Artificial Intelligence," *AI & SOCIETY* 40, no. 4 (2025): 3019–44, https://doi.org/10.1007/s00146-024-02050-7.

1. **EU and Member States officials must take the need to define and operationalize 'dual-use' seriously and establish clear metrics and parameters for the research and development of AI, as well as for its use**. Explicitly defining 'dual-use' is likely to stoke existing disagreements between the EU and Member States, who are wary of infringement on their national security. However, failing to define 'dual-use' properly threatens to undermine the AI Act's purpose and spirit. If we are to balance societal well-being with the needs of innovation, security, and defence, then the EU and Member State governments will have to move beyond referring to 'dual-use' as a catch-all term. They need to seriously discuss the risks that unchecked militarization poses to our societies and EU values.

2. Defining and operationalizing 'dual-use' will require a formal mechanism to address when a use-change occurs and when an AI system shifts between civilian and military contexts. **The EU should develop a notification mechanism, which would require developers and users to notify regulators when an AI system developed for or used in the civilian realm is repurposed or transformed for military use, or vice versa.** This mechanism would likewise trigger a regulatory reassessment, using the AI Act's risk framework to ensure the AI system has been properly classified and whether any change in status (i.e., exemption or inclusion from the Act's authority) is warranted.

These recommendations do not represent a panacea for the challenges discussed in this contribution. Rather, they are designed to address the messy nature of defining the boundaries of the civilian and military realms to not occlude AI systems from regulatory and political oversight in the name of national security and defence.



Emily Rand & LOTI / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Navigating China's Multi-Track Strategy in Global AI Governance

Hengfeng Zhao
University of Leeds, UK

Executive summary

Western engagement with China on AI governance currently faces a strategic mismatch. While the US and its allies often view China through a singular lens, Beijing employs domain-specific policy instruments: confronting technology restrictions, defending sovereign control, participating in safety norms, and leading the Global South. Treating these policy instruments as a uniform 'revisionist' drive produces policy miscalibration. Western capitals risk overreacting in safety forums where Chinese participation reduces global risk, while simultaneously under-reacting to the capacity-building initiatives that are reshaping the developing world's digital infrastructure. An effective Western strategy to engage with and deal with China requires compartmentalized responses. Policies must combine firmness on security and aggressive competition on development with institutionalized cooperation on existential risks.

Introduction

China's AI capacity-building represents the most consequential long-term challenge to Western influence in AI governance. At the same time, as this contribution argues, China does not pursue a single strategy when it comes to AI governance. Rather, it deploys distinct approaches depending on different governance domains. Western 'engage vs. contain' binaries treat China's AI approaches as uniform 'revisionism' and therefore miscalibrate policy responses. This contribution provides a critical assessment of this monolithic view, highlights China's policies across four contexts (hardware restrictions, data governance, AI safety summits, and capacity building in the Global South), and identifies recommendations for Western policymakers in each of these domains.

Note on terminology and coherence

This contribution discusses 'revisionism' as a label frequently applied in Western policy documents to describe Chinese behaviour, rather than as an objective descriptor. Similarly, terms like 'technological hegemony' are included to reflect Beijing's rhetorical framing of US policy. References to the 'Global South' denote the self-identified

coalition of developing nations as organized in the UN forums. ‘The West’ denotes North Atlantic Treaty Organization (NATO) and EU member states, as well as other states allied with the US.

This contribution assumes strategic coordination across Chinese ministries and state media. Some analysts may argue these approaches reflect internal fragmentation, tensions between security services seeking control and tech sectors needing openness, rather than centralized design. Even so, the external effects remain distinct, requiring the differentiated responses outlined below regardless of Beijing’s internal dynamics.

The problem: A monolithic view in a fragmented landscape

A central tension is paralyzing Western diplomacy regarding China’s AI ambitions. Western capitals predominantly view AI governance through the lens of national security and values competition, collapsing China’s diverse behaviours into a singular narrative of ‘revisionism’. Consequently, policy instruments, such as export controls and investment screening, are applied broadly across all domains.

This monolithic view is entrenched in Western strategic thought. UK government documents, such as *Strategic Competition in the Age of AI*, explicitly frame China’s AI advancements, including in predictive policing and military applications, as posing a challenge to the rules-based international order.[1] Similarly, EU parliamentary studies like *A New Era in EU-China Relations* frame China's growing assertiveness as a strategic challenge, echoing the US characterization of China as a ‘revisionist power’.[2] In the US, Department of Defense reports consistently describe China’s AI strategy as a tool for “revisionist power projection”,[3] a view echoed by Australian and Canadian

[1] James Black et al., *Strategic Competition in the Age of AI: Emerging Risks and Opportunities from Military Use of Artificial Intelligence* (RAND Corporation, 2024), prepared for UK Ministry of Defence and Foreign, Commonwealth and Development Office, https://www.gov.uk/government/publications/strategic-competition-in-the-age-of-ai-emerging-risks-and-opportunities-from-military-use-of-artificial-intelligence; see also UK Ministry of Defence, *Global Strategic Trends — The Future Starts Today* (2018): 36–42, https://www.gov.uk/government/publications/global-strategic-trends.

[2] Anna Saarela, *A New Era in EU-China Relations: More Wide-Ranging Strategic Cooperation?* (European Parliament, Policy Department for External Relations, 2018), https://www.europarl.europa.eu/RegData/etudes/STUD/2018/570493/EXPO_STU(2018)570493_EN.pdf; White House, *National Security Strategy of the United States of America* (2017), https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; see also European Parliament Think Tank, *Future Shocks 2023: Anticipating and Weathering the Next Storms* (2023), https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2023)751428.

[3] US Department of Defense, *Military and Security Developments Involving the People’s Republic of China* (2024), https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF; US Department of State, *The Elements of the China Challenge* (2020), https://www.state.gov/wp-content/uploads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf.

defence strategies, which identify China as a revisionist state eroding Western military advantages via AI.[4]

When Western actors treat distinct behaviours, such as commercial innovation or diplomatic norm-setting alongside military integration, as a single 'revisionist' drive, they risk two errors: overreacting in low-risk domains by rejecting Chinese participations in technical safety forums where their input is necessary for global risk reduction; and under-reacting in high-impact domains by failing to offer alternatives to China's capacity-building initiatives.

The broader context

Geopolitical competition has made AI a primary battlefield. Since late 2022, the US has pursued a "small yard, high fence" strategy,[5] restricting broad categories of advanced hardware. This approach peaked with the January 2025 "AI Diffusion Rule," which the Trump administration rescinded in May to cut rigid oversight mandates, while initially attempting to block access to specific performance tiers via new leakage controls.[6] This pivot reflected scepticism among US officials and European allies, who warn that trading containment for revenue risks eroding their national securities. With the EU designating economic security as a "first-order priority," European policymakers fear enforcing strict sector-wide controls at home while Washington pursues a divergent path that undercuts their shared strategic defence.[7]

---

[4] Australia's 2024 National Defence Strategy does not use the term 'revisionist' explicitly but frames China's military build-up as lacking 'strategic reassurance or transparency' and posing the most consequential risks to regional stability; earlier, the 2020 Defence Strategic Update described China's actions as creating the Indo-Pacific's "most consequential strategic realignment since the Second World War". Canada's 2024 defence policy update does not label China 'revisionist' directly but identifies it as a source of strategic competition and emphasizes AI-enabled threats to national security. See Department of Defence, *National Defence Strategy 2024* (Australian Government, 2024), https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program; Department of Defence, *2020 Defence Strategic Update* (Australian Government, 2020), https://www.defence.gov.au/about/strategic-planning/2020-defence-strategic-update; Government of Canada, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (Department of National Defence, 2024), https://www.canada.ca/en/department-national-defence/corporate/policies-standards/canada-defence-policy.html.

[5] The "small yard, high fence" strategy was articulated by then-US National Security Advisor Jake Sullivan. The American Presidency Project, "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution," April 27, 2023, https://www.presidency.ucsb.edu/documents/remarks-national-security-advisor-jake-sullivan-renewing-american-economic-leadership-the.

[6] Indeed, US policy grew volatile. By January 2026, it evolved into a transactional 'America First' model: authorizing advanced chip sales (like the H200) to approved Chinese entities for a 25% revenue cut, prioritizing economic leverage over the absolute denial of technology. See Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Guo Jiakun's Regular Press Conference on January 14, 2025," January 14, 2025, https://www.fmprc.gov.cn/eng/xw/fyrbt/lxjzh/202501/t20250114_11533650.html; Dara Kerr and Helen Davidson, "Trump Clears Way for Nvidia to Sell Powerful AI Chips to China," *The Guardian*, December 9, 2025, https://www.theguardian.com/technology/2025/dec/08/trump-nvidia-ai-chips-china; Alasdair Phillips-Robins, "Don't Panic Yet Over AI Chip Sales to China," *Carnegie Endowment for International Peace*, December 12, 2025, https://carnegieendowment.org/emissary/2025/12/china-ai-chip-sales-nvidia-trump; Peter Draper and Nathan Howard Gray, "With Nvidia's Second-Best AI Chips Headed for China, the US Shifts Priorities from Security to Trade," *The Conversation*, December 11, 2025, https://theconversation.com/with-nvidias-second-best-ai-chips-headed-for-china-the-us-shifts-priorities-from-security-to-trade-271831.

[7] Maria Demertzis, Alejandro Fiorito, and Konstantinos Panitsas, *Strategic Autonomy and European Competitiveness: Security Now Comes First* (European Parliament, 2025), https://www.europarl.europa.eu/RegData/etudes/STUD/2025/764371/ECTI_STU(2025)764371_EN.pdf.

In response, China accelerated its drive for technological self-reliance. A pivotal development was the release of DeepSeek-R1 large language model in early 2025, which achieved performance parity with leading US models at a fraction of the training cost—approximately $6 million for the base model compared to over $100 million for comparable US systems.[8] This efficiency challenged the assumption that US hardware dominance would permanently stifle Chinese innovation. Meanwhile, Beijing successfully led the adoption of UN General Assembly Resolution 78/311 in July 2024, diplomatically framing AI capacity building as a development right.[9]

We are at a critical juncture where technical breakthroughs have outpaced diplomatic manoeuvres. While the UK AI Safety Summit in November 2023 established a precedent for including China in high-level safety discussions, the subsequent bifurcation of hardware supply chains and development standards threatens to create incompatible AI ecosystems fragmented along geopolitical lines.[10]

China's four-fold AI governance repertoire

China's behaviour is best understood as four distinct strategies for managing its global standing.

Approach I: Confronting technology restrictions

Context: Hardware restrictions, export controls, and computing power.

When facing containment measures regarding AI chips, China adopts a confrontational stance. It does not merely evade sanctions; it actively challenges the legitimacy of the US-led global order. China reframes security measures adopted by the US as 'hegemonic' acts designed to suppress development rights.

This was evident after the Trump administration's rescission of the Biden-era AI Diffusion Rule and subsequent shifts toward transactional chip export policies in 2025. The Chinese Foreign Ministry characterized US moves as a "stumbling block strategy" intended to deprive developing countries of technological progress.[11] Furthermore,

[8] Alex He, *AI Development and Governance in China amid Geopolitical Tensions*, CIGI Paper No. 338 (Centre for International Governance Innovation, 2025), https://www.cigionline.org/publications/ai-development-and-governance-in-china-amid-geopolitical-tensions/; Global Times, "DeepSeek Proves 'Small Yard, High Fence' Cannot Hinder Innovation: Global Times Editorial," February 5, 2025, https://www.globaltimes.cn/page/202502/1327847.shtml.

[9] United Nations General Assembly, "Resolution Adopted by the General Assembly: Enhancing International Cooperation on Capacity-Building of Artificial Intelligence (A/RES/78/311)," July 5, 2024, https://docs.un.org/en/A/res/78/311.

[10] He, *AI Development and Governance in China*, 12.

[11] The phrase "stumbling block strategy" translates the Chinese 绊脚石战略 directly, whereas the website's English version employs different terminology. See Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Guo Jiakun's Regular Press Conference on January 14, 2025."

Chinese state media leveraged the success of DeepSeek to argue that US containment is futile, asserting that technological breakthroughs will "inevitably overcome political barriers" and that restrictions effectively force Chinese efficiency.[12]

In this domain, Beijing's strategy is to delegitimize restrictions beyond evasion, embodying a broader critique of US technological hegemony.

Approach II: Defending sovereign control

Context: Data governance, censorship, and domestic regulation.

In the realm of ethics and internal regulation, China rejects the universal application of liberal democratic norms. Instead, it asserts that AI governance must respect "national conditions" and "national sovereignty".[13] This allows Beijing to defend its domestic censorship regime while presenting it internationally as a defence of sovereign rights against foreign interference.

In the Global AI Governance Initiative 2023, China emphasized that governance must be "based on respect for sovereignty" and opposed "using AI to interfere in other countries' internal affairs".[14] This stance appeals to nations wary of Western tech giants' influence. Regarding data security, China argues that states should not harvest data from other countries without permission, framing its strict data localization laws as protection against "technological hegemony" and "long-arm jurisdiction".[15]

By grounding its domestic controls in the language of sovereignty, Beijing positions censorship not as authoritarianism but as resistance to foreign interference, a framing that likely resonates with states wary of Western tech dominance.

Approach III: Participating in global safety norms

Context: Existential risk, AI safety standards, and global summits.

Contradicting its combative stance on hardware, China actively seeks inclusion in established international forums regarding AI safety. Here, Beijing aims to be

[12] See Global Times, "DeepSeek Proves 'Small Yard, High Fence' Cannot Hinder Innovation". China's claims about the futility of containment warrant scepticism: DeepSeek "relied heavily on Nvidia's advanced AI chips" (specifically the H800) and its success "may be the exception rather than the norm". See He, *AI Development and Governance in China*, 7.

[13] Permanent Mission of the People's Republic of China to the UN, "Global AI Governance Action Plan," July 26, 2025, https://un.china-mission.gov.cn/eng/zgyw/202507/t20250729_11679232.htm.

[14] Ministry of Foreign Affairs of the People's Republic of China, "Global AI Governance Initiative," October 20, 2023, https://www.fmprc.gov.cn/eng/xw/zyxw/202405/t20240530_11332389.html.

[15] Xinhua, "U.S. Hegemony and Its Perils," February 20, 2023, https://english.news.cn/20230220/1b9a2c2bcfb742ad872c58ddda549374/c.html; Zhou Jing and Sun Nanxiang, "汇聚完善全球数字治理的强大合力" [Gathering Powerful Synergy to Improve Global Digital Governance], *People's Daily*, November 27, 2025, accessed via Xinhuanet, http://www.news.cn/politics/20251127/f35797db0b98478d804b75ba12882b08/c.html; Ministry of Foreign Affairs of the People's Republic of China, "US Hegemony and Its Perils," February 20, 2023, https://www.mfa.gov.cn/eng/zy/gb/202405/t20240531_11367483.html.

recognized as a ‘responsible major power’, a rule-maker, and a necessary partner in managing catastrophic risks.

China’s high-level participation in the UK AI Safety Summit (Bletchley Park) in November 2023 was pivotal. Vice Minister of Science and Technology Wu Zhaohui led a delegation that emphasized Beijing’s willingness to “pool wisdom” for a governance framework.[16] Similarly, the establishment of intergovernmental AI talks with the US demonstrates China’s desire to shape global rules from the inside rather than being isolated.[17]

This cooperative posture stands in contrast to Beijing’s confrontational stance on hardware. China seeks recognition from established standard-setters, calibrating its approach based on whether it perceives the governance domain as threatening or legitimizing.

Approach IV: Leading the Global South

Context: Capacity building and the UN development agenda.

China is aggressively pivoting to the Global South, framing the ‘AI divide’ as a human rights issue. Beijing contrasts its ‘inclusive’ approach with Western ‘exclusivity’, employing universalist language (“Shared Future,” “AI for All”) to build a coalition of developing nations.[18]

This is exemplified by China’s *AI Capacity-Building Action Plan for Good and for All*, launched in September 2024. The plan promises infrastructure connectivity and personnel training to bridge the “intelligence gap”.[19] However, China’s traction varies regionally; while its infrastructure-first approach has found strong success in Central Asia, Southeast Asia, and parts of Africa, it faces competition and scepticism in and Latin America.[20]

[16] Yang Sheng and Qi Xijia, “China to Pool Wisdom for AI Governance Framework in UK,” *Global Times*, November 1, 2023, https://www.globaltimes.cn/page/202311/1301030.shtml.
[17] Ma Jingjing and Tao Mingyang, “US Urged to Correct Mistakes, Work with China for Win-Win Results as the Two Nations Agree to Hold Government Talks on AI,” *Global Times*, November 16, 2023, https://www.globaltimes.cn/page/202311/1301984.shtml.
[18] Ministry of Foreign Affairs of the People’s Republic of China, “AI Capacity-Building Action Plan for Good and for All,” September 27, 2024, https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/AI/202412/t20241218_11497486.html; https://www.mfa.gov.cn/web/wjbzhd/202409/t20240927_11498463.shtml.
[19] Ibid.
[20] Jing Cheng and Jinghan Zeng, “Shaping AI’s Future? China in Global AI Governance,” *Journal of Contemporary China* 32, no. 143 (2023): 794–810; https://doi.org/10.1080/10670564.2022.2107391; Jennifer Bouey et al., *China’s AI Exports: Developing a Tool to Track Chinese Development Finance in the Global South–Technical Documentation* (RAND Corporation, 2023), https://www.rand.org/t/RRA2696-1; Jennifer Bouey et al., *China’s AI Exports Database (CAIED)* (RAND Corporation, 2025), https://www.rand.org/pubs/tools/TLA2696-1.html; Richard Heeks et al., “China’s Digital Expansion in the Global South: Systematic Literature Review and Future Research Agenda,” *The Information Society* 40, no. 2 (2024): 69–95; https://doi.org/10.1080/01972243.2024.2315875.

This capacity-building offensive represents Beijing's most consequential long-term play. By providing the infrastructure for developing nations' AI transitions, China embeds its technical standards and cultivates diplomatic alignment for decades to come.

China's four strategic postures: An overview

China's four approaches emerge from two underlying dimensions: whether Beijing seeks integration with or differentiation from the existing order, and whether it accepts or challenges dominant standards (Table 2). These approaches vary depending on the governance domain (Table 3).

Table 2. China's Strategic Positioning in AI Governance

	Seeks integration	**Seeks differentiation**
Accepts dominant standards	**Approach III: Participation** (Safety forums: seeks peer recognition)	**Approach II: Sovereignty** (Data governance: asserts equivalent legitimacy)
Challenges dominant standards	**Approach IV: Leadership** (Global South: builds alternative coalition)	**Approach I: Confrontation** (Hardware: delegitimizes restrictions)

Source: author

Conclusion

China's multi-track approach to AI governance is calibrated. Beijing confronts where it perceives illegitimate constraint, defends where it prioritizes domestic control, cooperates where it seeks status, and leads where it sees opportunity. Western policymakers who flatten these into a single 'revisionist' narrative will miscalibrate their responses, ceding ground in the Global South while overreacting in safety forums where Chinese participation could reduce global risk. The window for differentiated engagement is narrowing. As AI capabilities advance and governance frameworks harden, the strategic choices made in the next two years will shape the international order for decades.

Recommendations

To effectively navigate China's multi-track strategy on AI governance, Western policymakers should adopt a differentiated approach, reflecting the different contexts. This contribution recommends that Western policymakers:

1. **Reframe export controls as targeted security measures.** China frames Western restrictions as an attempt to block global progress. When imposing restrictions, US and European policymakers should:
    a. Publish specific risk assessments that identify the military applications and privacy risks they aim to prevent, rather than targeting broad technology categories.
    b. Maintain open commercial AI trade channels and publicize them to debunk the 'decoupling' narrative.
    c. Acknowledge Chinese technical achievements directly, as credibility requires admitting DeepSeek's efficiency breakthrough while highlighting the governance divergence regarding how such tools are used for surveillance.[21]

2. **Institutionalize safety cooperation.** China is seeking admission to the global rule-making club. Western diplomats should facilitate China's integration into technical safety bodies but make participation conditional on specific transparency measures. These include (1) incident reporting protocols (mandatory alerts for model failures), (2) third-party red-teaming access (allowing independent experts to test models for dangerous flaws), and (3) the pre-registration of frontier training runs (notifying international bodies before training massive AI systems above a specific computing power). These engagements should be technical and depoliticized, focusing on shared risks like model collapse or bioterrorism enablement.

3. **Compete on capacity building.** China is offering tangible AI development aid in the Global South.[22] The US State Department's new Bureau of Cyberspace and Digital Policy, together with the EU's Global Gateway, should jointly establish a dedicated financing facility for AI infrastructure. This initiative must rival Beijing's Global South capacity-building offensive by offering financing for compute infrastructure and open-source model training for developing nations. If the West does not provide the infrastructure for the AI transition, China will embed its technical standards for decades to come.

4. **Engage data sovereignty concerns without endorsing surveillance.** Policymakers should acknowledge legitimate data sovereignty concerns, which many European and Global South nations share regarding US tech giants but distinguish them from human rights violations. Forums like the Organisation for Economic Co-operation and Development (OECD), the G20, and UN

[21] He, *AI Development and Governance in China*, 5; Esther Goreichy, Abigaël Vasselier, and Grzegorz Stec, *Profiling European Countries' Resilience towards China - 2025 Update* (MERICS, 2025), https://merics.org/en/report/profiling-european-countries-resilience-towards-china-2025-update.
[22] He, *AI Development and Governance in China*, 18-19; Concordia AI, "AI Safety in China #17," *AI Safety in China*, October 24, 2024, https://aisafetychina.substack.com/p/ai-safety-in-china-17; Bouey et al., *China's AI Exports.*

specialized agencies (like the ITU) should host technical dialogues on cross-border data flows and privacy-enhancing technologies to find technical common ground.[23] This allows for cooperation on data governance frameworks without endorsing Beijing's model of state surveillance.

Table 3. Policy Implications of China's Positioning in AI Governance by Domain

Approach	Domain	China's posture	Western leverage
Confrontation	Hardware/Chips	Challenge legitimacy of restrictions	Limited: reframe export controls as targeted security measures
Sovereignty	Data/Ethics	Assert sovereign equivalence	Engage data sovereignty
Participation	Safety/Risk	Seek inclusion; act as responsible peer	High: institutionalize safety cooperation, condition on transparency
Leadership	Global South	Build coalition; offer infrastructure	Critical: compete on capacity building

Source: author

Acknowledgements

I would like to express my sincere gratitude to Anna Nadibaidze and Justinas Lingevičius for their insightful and constructive suggestions on earlier drafts of this brief. I also appreciate the valuable feedback received during the EISA Early Career Researchers Workshop 2025 in Bologna.

[23] Huw Roberts et al., "Global AI Governance: Barriers and Pathways Forward," *International Affairs* 100, no. 3 (2025): 1275–1286, https://doi.org/10.1093/ia/iiae073.

Sinem Görücü / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

About the Contributors

Anna Nadibaidze is a postdoctoral researcher in International Politics at the Center for War Studies, University of Southern Denmark. Her research examines artificial intelligence in international security and the governance of AI in the military domain.

Benjamin T. Johnson is an assistant professor of Humane Artificial Intelligence and International Relations with the Department of International Relations and International Organization at the University of Groningen, Netherlands. His primary research areas include the implications of AI for international politics, society, and security, as well as Arctic security and defence.

Elena Kavanagh is a legal scholar and research affiliate at the Centre for the Study of Existential Risk, University of Cambridge. Her work focuses on AI governance, Indigenous rights, and global power asymmetries, with particular expertise in decolonial and pluralistic approaches to technology policy.

Hengfeng Zhao is a PhD candidate at the University of Leeds, specializing in International Relations. His research focuses on illiberalism, norm contestation, and IR theories. His work has been published in *Global Studies Quarterly* and explores Global South perspectives on international norms.

Justinas Lingevicius leads the Politics of Technology research group at the Institute of International Relations and Political Science, Vilnius University. His research focuses on the politics of emerging technologies and security, with particular attention to the EU and the Baltic region.

Qiaochu Zhang is a Max Weber Fellow at the European University Institute. Prior to this, she was a postdoctoral researcher on the AutoNorms project at University of Southern Denmark. Her current research examines China's approaches to global AI governance.

Robin Vanderborght is a postdoctoral researcher in International Relations at the University of Antwerp. He is currently working on a project that examines the impact of European technology startups on the norms and conduct of (algorithmic) warfare.

Stefka Schmid is a postdoctoral researcher at the Digital Economic Security Lab (DIESL) at Aalto University, Finland. She studies the geopolitics of cloud computing, with a focus on state-industry relations. Her academic work also includes analyses of governmental visions of AI as well as human-computer interaction in crisis scenarios.

Center for War Studies
University of Southern Denmark
Campusvej 55
Odense M 5230
Denmark

Phone: +45 6550 1000
sdu@sdu.dk
www.sdu.dk