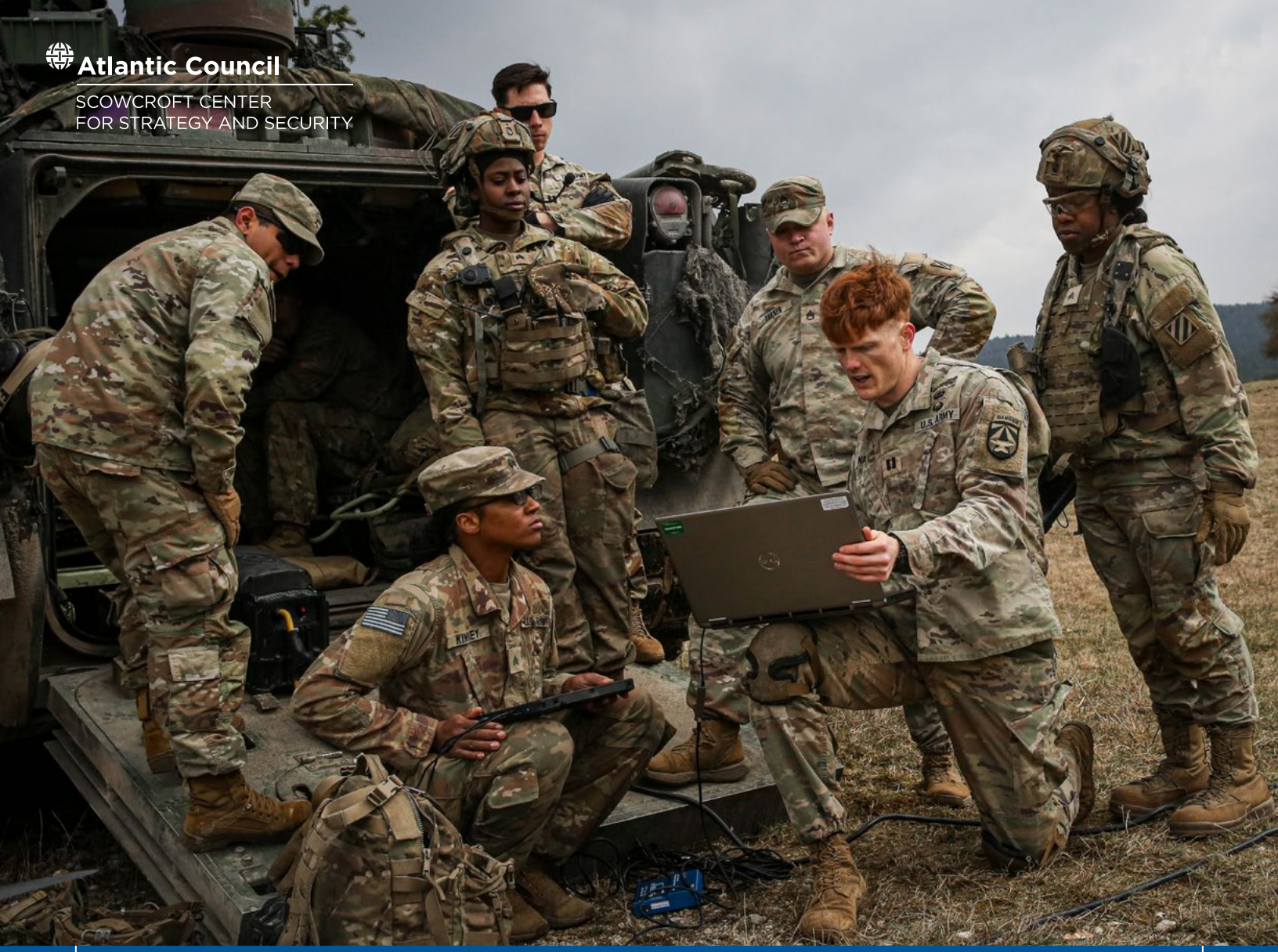
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY



SECOND-ORDER IMPACTS OF CIVIL ARTIFICIAL INTELLIGENCE REGULATION ON DEFENSE:

Why the national security community must engage

By Deborah Cheverton

Forward Defense (*F*D):

Forward Defense, housed within the Scowcroft Center for Strategy and Security, generates ideas and connects stakeholders in the defense ecosystem to promote an enduring military advantage for the United States, its allies, and partners. Our work identifies the defense strategies, capabilities, and resources the United States needs to deter and, if necessary, prevail in future conflict.

Scowcroft Center for Strategy and Security:

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The author would like to thank PrimerAI for its generous support in sponsoring this paper.

Cover

US Army soldiers assigned to the Artificial Intelligence Integration Center conduct drone test flights and software troubleshooting during an exercise for NATO allies and partners in Germany.

Source: Spc. Micah Wilson/US Army

ISBN-13: 978-1-61977-506-0

June 2025

Atlantic Council
1400 L Street NW, 11th Floor

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Second-order impacts of civil artificial intelligence regulation on defense:

Why the national security community must engage

By Deborah Cheverton

Table of contents

AI civil governance and defense: Unintended consequences and the call to engage

1: EXECUTIVE SUMMARY

Civil regulation of artificial intelligence (AI) is hugely complex and evolving quickly, with even otherwise well-aligned countries taking significantly different approaches. At first glance, little in the content of these regulations is directly applicable to the defense and national security community. The most wide-ranging and robust regulatory frameworks have specific carve-outs that exclude military and related use cases. And while governments are not blind to the need for regulations on AI used in national security and defense, these are largely detached from the wider civil AI regulation debate. However, when potential second-order or unintended consequences on defense from civil AI regulation are considered, it becomes clear that the defense and security community cannot afford to think itself special. Carve-out boundaries can, at best, be porous when the technology is inherently dual use in nature. This paper identifies three broad areas in which this porosity might have a negative impact, including

- market-shaping civil regulation that could affect the tools available to the defense and national security community;
- judicial interpretation of civil regulations that could impact the defense and national security community's license to operate; and
- regulations that could add additional cost or risk to developing and deploying AI systems for defense and national security.

This paper employs these areas as lenses through which to assess civil regulatory frameworks for AI to identify which initiatives should concern the defense and national security community. These areas are grouped by the level of resources and attention that should be applied while the civil regulatory landscape continues to develop. Private-sector AI firms with dual-use products, industry groups, government offices with national security responsibility for AI, and legislative staff should use this paper as a roadmap to understand the impact of civil AI regulation on their equities and plan to inject their perspectives into the debate.

BE SUPPORTIVE

Areas or initiatives that the community should get behind and support in the short term

Technical standards	Defense and national security technical standards should, as far as possible, align with civil-sector standards to minimize the cost of compliance, maximize interoperability, and allow efficient adoption of civil solutions to specialist problems. ACTION ON: **chief information officers, chief AI officers, standard-setting bodies, and AI developers in the public and private sectors.**
Risk-assessment tools	Adopting tools and best practices developed in the civil sector could save time and money that could be better spent on advancing capability or readiness. ACTION ON: **chief information officers, chief AI officers, and risk-management professionals including auditors, system integrators, and AI developers in the public and private sectors.**
Safety and assurance tools	As above, adopting tools and best practices developed in the civil sector could be more efficient, but there could also be reputational and operational benefits to equivalency in some areas like aviation, in which military and civil users of AI systems might need to share airspace. ACTION ON: **chief information officers, chief AI officers, compliance officers, and domain safety specialists.**

BE PROACTIVE

Areas that are still maturing but in which greater input is needed and the impact on the community could be significant in the medium term

Regulation of adjacent sectors and use cases	Restrictions on the use of AI in domestic security and policing could limit development of capabilities of use to the defense and national security community or increase the cost of capabilities by limiting economies of scale. This is especially concerning in technically complex areas such as counterterrorism, covert surveillance and monitoring, and pattern detection for intelligence purposes. ACTION ON: **chief information officers, chief AI officers, legal and operational policy advisers, and AI developers in the public and private sectors.**
Data sharing and transfer	Regulatory approaches that impact, in policy or practical terms, the ability of the defense and national security community to share data between allies across national borders could limit or impose additional costs on collaborative capability development and deployment. ACTION ON: **chief information officers, chief AI officers, data-management specialists, and export-control policymakers.**
Special regulatory provisions for generative AI	Regulations placed on the general-purpose AI systems that underpin sector-specific applications could impact the capabilities available to defense and national security users, even if those use cases are themselves technically exempt from such restrictions. ACTION ON: **chief information officers, chief AI officers, standard-setting bodies, legal and operational policy advisers, and AI developers in the public and private sectors.**

BE WATCHFUL

Areas that are still maturing but in which uncertain future impacts could require the community's input

Licensing and registration databases	Such databases could easily exclude algorithms and models developed specifically for defense or national security purposes. However, registering the open-source or proprietary models on which those tools are based could still pose a security risk if malign actors accessed the registry. ACTION ON: **chief information officers, chief AI officers, risk-management professionals, and counterintelligence and security policymakers.**
Data protection, privacy, and copyright regulations	AI systems do not work without data. Domestic regulation of privacy, security, and rights-impacting data, as well as interpretations of fair use in existing copyright law, could limit access to training data for future AI systems. ACTION ON: **chief information officers, chief AI officers, privacy and data-protection professionals, and AI developers in the public and private sectors.**
Market-shaping regulation	The AI industry, especially at the cutting edge of general-purpose AI, is heavily dominated by a few incumbents, most of which operate internationally. Changes to the substance or interpretation of domestic antitrust regulations could impact the supply base available to the defense and national security community. ACTION ON: **chief information officers, chief AI officers, commercial policymakers, and legal advisers.**
Legal liability	Like any other capability, AI systems used by the military and national security community in an operational context are covered by the law of armed conflict and broader international humanitarian law, not domestic legislation. However, in nonoperational contexts, judicial interpretation of civil laws could impact particularly questions of criminal, contractual, or other liability. ACTION ON: **chief information officers, chief AI officers, and legal and operational policy advisers.**

2: INTRODUCTION

"AI is an exciting technology that will boost our productivity and facilitate a new approach to work, leisure, and everything else."

"No, AI is a terrifying technology that poses an existential threat to human society and possibly to life itself."

Whichever side of this argument—or the gray and murky middle ground—one tends toward, it is clear that artificial intelligence (AI) is an enormously consequential technology in at least two ways. First, the AI revolution will change the way people work, live, and play. Second, the development and adoption of AI will transform the way future wars are fought, particularly in the context of US strategic competition with China. These conclusions, brought to the fore by the seemingly revolutionary advances in generative AI—as typified by ChatGPT and other large multimodal models—are natural conclusions drawn from decades of incremental advances in basic science and digital technologies. As public interest in AI and fears of its misuse rise, governments have started to regulate it.

Much like AI itself, the global discussion on how best to regulate AI is complex and fast-changing, with big differences in approach seen even between otherwise well-aligned countries. Since the Organisation for Economic Co-operation and Development (OECD) published the first internationally agreed-upon set of principles for the responsible and trustworthy development of AI policies in 2019, the organization has identified more than 930 AI-related policy initiatives across 70 jurisdictions. The comparative analysis presented here reveals huge variation across these initiatives, which range from comprehensive legislation like the European Union (EU) AI Act to loosely managed voluntary codes of conduct, like that agreed to between the Biden administration and US technology companies. Most of the initiatives aim to improve the ability of their respective countries to thrive in the AI age; some aim to reduce the capacity of their competitors to do the same. Some take a horizontal approach focusing on specific sectors, use cases, or risk profiles, while others look vertically at specific kinds of AI systems, and some try to do bits of both. Issues around skills, supply chains, training data, and algorithm development feature varying degrees of emphasis. Almost all place some degree of responsibility on developers of AI systems, albeit voluntarily in the loosest arrangements, but knotty problems around accountability and enforcement remain.

The defense and national security community has largely kept itself separate from the ongoing debates around civil AI regulation, focusing instead on internally directed standards and processes. The unspoken assumption seems to be that regulatory carve-outs or special considerations will insulate the community, but that view fails to consider the potential second-order implications of civil regulation, which will be market shaping and will affect a whole swath of areas in which defense has significant equity. Furthermore, the race to develop AI tools is itself now an arena of geopolitical competition with strategic consequences for defense and security, with the ability to intensify rivalries, shift economic and technological advantage, and shape new global norms. Relying on regulatory carve-outs for the development and use of AI in defense is likely to prove ineffective at best, and could seriously limit the ability of the United States and its allies to reap the rewards that AI offers as an enhancement to military capabilities on and off the battlefield.

This paper provides a comparative analysis of the national and international regulatory initiatives that will likely be important for defense and national security, including initiatives in the United States, United Kingdom (UK), European Union, China, and Singapore, as well as the United Nations (UN), OECD, and the Group of Seven (G7). The paper assesses the potential implications of civil AI regulation on the defense and national security community by grouping them into three buckets.

- **Be supportive:** Areas or initiatives that the community should get behind and support in the short term.
- **Be proactive:** Areas that are still maturing but in which greater input is needed and the impact on the community could be significant in the medium term.
- **Be watchful:** Areas that are still maturing but in which uncertain future impacts could require the community's input.

3: DEFINITIONS

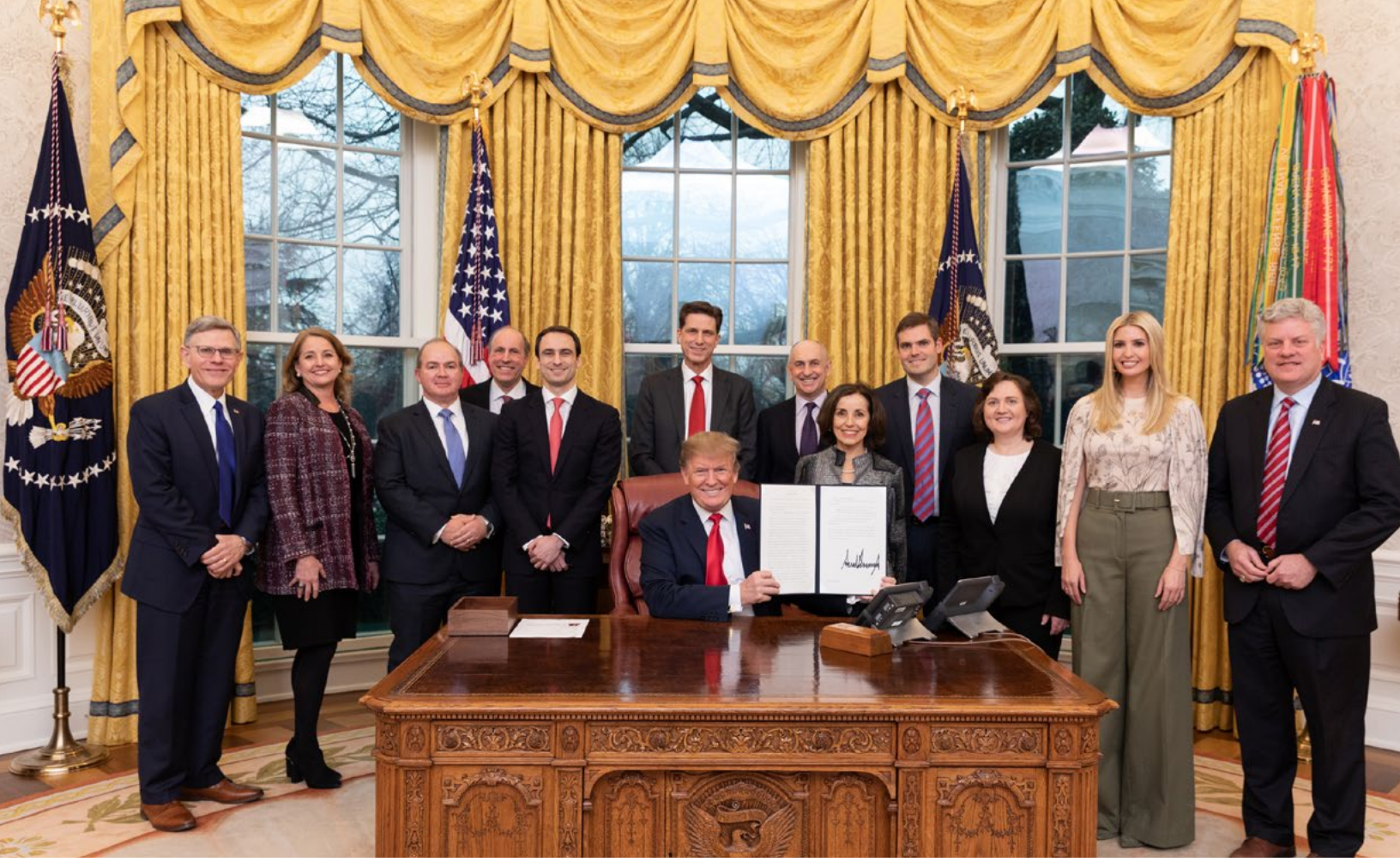
To properly survey the international landscape, this paper takes a relatively expansive view of regulation and what constitutes an AI system.

The former is usually understood by legal professionals to mean government intervention in the private domain or a legal rule that implements such intervention.[1] In this context, that definition would limit consideration to so-called "hard regulation," largely comprising legislation and rules enforced by some kind of government organization, and would exclude softer forms of regulation such as voluntary codes of conduct and non-enforceable frameworks for risk assessment and classification. For this reason, this paper interprets regulation more loosely to mean the controlling of an activity or process, usually by means of rules, but not necessarily deriving from government action or subject to formal enforcement mechanisms. When in doubt, if a policy or regulation says it is aimed at controlling the development of AI, this paper takes it at its word.

To define AI, this paper follows the National Artificial Intelligence Act of 2020, as enacted via the 2021 National Defense Authorization Act, which defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."[2] This definition neatly encompasses the current cutting edge of narrow AI systems based on machine learning. At a later date, it might also be expected to include theorized, but not yet realized, artificial general intelligence or artificial superintelligence systems. This paper deliberately excludes efforts to control the production of advanced microchips as a precursor technology to AI, as there is already significant research and commentary on that issue.

1 Barak Orbach, "What Is Regulation?" *Yale Journal on Regulation*, July 25, 2016, https://www.yalejreg.com/bulletin/what-is-regulation/.

2 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, PubL. 116-283.PS, 134 STAT. 3388 (2021) https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf.



US President Donald Trump signs an executive order on “Maintaining American Leadership in Artificial Intelligence” in 2019.
Source: White House

4: NATIONAL AND SUPRANATIONAL REGULATORY INITIATIVES

4.1 United States

Thus far, the US approach to AI regulation can perhaps best be characterized as a patchwork attempting to balance public safety and civil rights concerns with a widespread assumption that US technology companies must be allowed to innovate for the country to succeed. There is consensus that government must play a regulatory role, but a wide range of opinions on what that role should look like.

4.1.1 Overview

Regulatory approach

Overall, the regulatory approach is technology agnostic and focused on specific use cases, especially those relating to civil liberties, data privacy, and consumer protection.

It should be supplemented in some jurisdictions by additional guidelines for models that are thought to present particularly severe or novel risks. The latter includes generative AI and dual-use foundation models.

Scope of regulation

Focus on outcomes generated by AI systems with limited consideration of individual models or algorithms, except dual-use foundation model elements that use a compute-power threshold definition.

At the federal level, heads of government agencies are individually responsible for the use of AI within their organizations, including third-party products and services. This includes training data, with particular focus on the use of data that are safety, rights, or privacy impacting as defined in existing regulation.

Type of regulation

At the federal level, regulation should entail voluntary arrangements with industry and incorporation of AI-specific issues into existing hard regulation through adapting standards, risk management, and governance frameworks.

Some states have put in place bespoke hard regulation of AI, including disclosure requirements, but this is generally focused on protecting existing consumer and civil rights regimes.

Target of regulation

At the federal level, voluntary arrangements are aimed at developers and deployers of AI-enabled systems and intended to protect the users of those systems, with particular focus on public services provided by or through federal agencies. Service providers might not be covered due to Section 230 of the Communications Act.

At the state level, some legislatures have placed more specific regulatory requirements on developers and deployers of AI-enabled systems to their populations, but the landscape is uneven and evolving.

Coverage of defense and national security

Defense and national security are covered by separate regulations at the federal level, with bespoke frameworks for different components of the community. State-level regulation does not yet incorporate sector-specific use cases, but domestic policing, counterterrorism, and the National Guard could fall under future initiatives.

4.1.2 Federal regulation

At the federal level, AI has been a rare area of bipartisan interest and relative agreement in recent years. The ideas raised in 2018 by then President Donald Trump in Executive Order (EO) 13845 can be traced through subsequent Biden-era initiatives, including voluntary commitments to manage the risks posed by AI, which were agreed upon with leading technology companies in mid-2023.[3] However, other elements of the Biden approach to AI—such as the 2022 Blueprint for an AI Bill of Rights, which focused on potential civil rights harms of AI, and the more recent EO14110 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence—were unlikely to survive long, with the latter explicitly called out for reversal in the 2024 Republican platform.[4] Trump was able to follow through on this easily because, while EO14110 was a sweeping document that gave elements of the federal government 110 specific tasks, it was not law and was swiftly overturned.[5]

While EO14110 was revoked, it is not clear what might replace it.[6] It seems likely that the Biden administration's focus on protecting civil rights as laid out by the Office of Management and Budget (OMB) will become less prominent, but the political calculus is complicated and revising Biden-era AI regulation is not likely to be at the top of the Trump administration's to-do list.[7] So, the change of administration does not necessarily mean that all initiatives set in motion by Biden will halt.[8] Before EO14110 was issued, at least a dozen federal agencies had already issued guidance on the use of AI in their jurisdictions and more have since followed suit.[9] These may well survive, especially the more technocratic elements like the National Institute of Standards and Technology's Artificial Intelligence Risk Management Framework (NIST Framework), which is due to be expanded to cover risks that are novel to, or exacerbated by, the use of generative AI.[10] The NIST Framework, along with guidance on secure software development practices related to training data for generative AI and dual-use foundation models, and a plan for global engagement on AI standards, are voluntary tools and generally politically uncontentious.[11]

---

3 The other EOs overridden by President Biden were: EO13859 Maintaining American Leadership in Artificial Intelligence and EO13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. "Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI," White House, press release, July 21, 2023, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

4 "AI Bill of Rights Making Automated Systems Work for the American People," White House, October 2022, https://marketingstorageragrs.blob.core.windows.net/webfiles/Blueprint-for-an-AI-Bill-of-Rights.pdf; "RNC 2024 Platform," Republican National Committee, July 8, 2024, https://www.presidency.ucsb.edu/documents/2024-republican-party-platform.

5 Ronnie Kinoshita, Luke Koslosky, and Tessa Baker, "The Executive Order on Safe, Secure, and Trustworthy AI: Decoding Biden's AI Policy Roadmap," Center for Security and Emerging Technology, May 3, 2024, https://cset.georgetown.edu/article/eo-14410-on-safe-secure-and-trustworthy-ai-trackers.

6 Jeff Tollefson, et al., "What Trump's Election Win Could Mean for AI, Climate and Health," *Nature*, November 8, 2024, https://www.nature.com/articles/d41586-024-03667-w; Gyana Swain, "Trump Taps Sriram Krishnan for AI Advisor Role amid Strategic Shift in Tech Policy," CIO, December 23, 2024, https://ramaonhealthcare.com/trump-taps-sriram-krishnan-for-ai-advisor-role-amid-strategic-shift-in-tech-policy/.

7 Trump's allies are divided on AI. While Trump himself is friendly to the AI industry, polling shows that many Americans are worried about the impact on their jobs. Julie Ray, "Americans Express Real Concerns about Artificial Intelligence," Gallup, August 27, 2024, https://news.gallup.com/poll/648953/americans-express-real-concerns-artificial-intelligence.aspx.

8 "OMB Releases Final Guidance Memo on the Government's Use of AI," Crowell & Moring, April 9, 2024, https://www.crowell.com/en/insights/client-alerts/omb-releases-final-guidance-memo-on-the-governments-use-of-ai; Gabby Miller and Justin Hendrix, "Where US Tech Policy May Be Headed during a Second Trump Term," Tech Policy Press, November 7, 2024, https://www.techpolicy.press/where-us-tech-policy-may-be-headed-during-a-second-trump-term/; Harry Booth and Tharin Pillay, "What Donald Trump's Win Means for AI," Time, November 8, 2024, https://time.com/7174210/what-donald-trump-win-means-for-ai.

9 Ellen Glover, "AI Bill of Rights: What You Should Know," Built In, March 19, 2024, https://builtin.com/artificial-intelligence/ai-bill-of-rights.

10 "AI Risk Management Framework. Artificial Intelligence Risk Management Framework (AI RMF 1.0)," National Institute of Standards and Technology, 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf; "Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile," National Institute of Standards and Technology, 2024, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf.

11 Harold Booth, et al., "Secure Software Development Practices for Generative AI and Dual-Use Foundation Models," National Institute of Standards and Technology, April 2024, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf; Jesse Dunietz, et al., "A Plan for Global Engagement on AI Standards," National Institute of Standards and Technology, 2024, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-5.pdf.

In Congress, then-Senate Majority Leader Chuck Schumer (D-NY) led the AI charge with a program of educational Insight Forums, which led to the Bipartisan Senate AI Working Group's Roadmap for AI Policy.[12] Some areas of the roadmap support the Biden administration's approach, most notably support for NIST, but overall it is more concerned with strengthening the US position vis-à-vis international competitors than it is with domestic regulation.[13] No significant legislation on AI is on the horizon, and the roadmap's level of ambition is likely constrained by dynamics in the House of Representatives, given that Speaker Mike Johnson is on the record arguing against overregulation of AI companies.[14] A rolling set of smaller legislative changes is more likely than an omnibus AI bill, and the result will almost certainly be a regulatory regime more complex and distributed than that in the EU.[15] This can already be seen in the defense sector, where the 2024 National Defense Authorization Act (NDAA) references AI 196 times and includes provisions on public procurement of AI, which were first introduced in the Advancing American AI Act.[16] These provisions require the Department of Defense (DoD) to develop and implement processes to assess its ethical and responsible use of AI and a study analyzing vulnerabilities in AI-enabled military applications.[17]

Beyond the 2024 NDAA, the direction of travel in the national security space is less clear. The recently published National Security Memorandum (AI NSM) seemingly aligns with Trump's worldview.[18] Its stated aims are threefold: first, to maintain US leadership in the development of frontier AI systems; second, to facilitate adoption of those systems by the national security community; and third, to build stable and responsible frameworks for international AI governance.[19] The AI NSM supplements self-imposed regulatory frameworks already published by the DoD and the Office of the Director of National Intelligence. But, unlike those existing frameworks, the AI NSM is almost exclusively concerned with frontier AI models.[20] The AI NSM mandates a whole range of what it calls "deliberate and meaningful changes" to the ways in which the US national security community deals with AI, including significant elevation in power and authority for chief AI officers across the community.[21] However, the vast majority of restrictive provisions are found in the supplementary Framework to Advance AI Governance and Risk Management in National Security, which takes an EU-style, risk-based approach with a short list of prohibited uses (including the nuclear firing chain), a longer list of "high-impact" uses that are permitted with greater oversight, and robust minimum-risk management practices to include pre-deployment risk assessments.[22] Comparability with EU regulation is unlikely to endear the AI NSM to Trump, but it is interesting to note that Biden's National Security Advisor Jake Sullivan argued that restrictive provisions for AI safety, security, and trustworthiness are key components of expediting deliver-

12 The Insight Forums took input from experts in the field on subjects ranging from workforce implications and copyright concerns to doomsday scenarios and questions around legal liability. Gabby Miller, "US Senate AI 'Insight Forum' Tracker," Tech Policy Press, December 8, 2023, https://www.techpolicy.press/us-senate-ai-insight-forum-tracker.

13 Chuck Schumer, et al., "Driving US Innovation in Artificial Intelligence," US Senate, May 15, 2024, https://www.schumer.senate.gov/imo/media/doc/Roadmap_Electronic1.32pm.pdf.

14 The House of Representatives AI Task Force Report was published too late for inclusion in this paper. Prithvi Iyer and Justin Hendrix, "Reactions to the Bipartisan US House AI Task Force Report," Tech Policy Press, December 20, 2024, https://www.techpolicy.press/reactions-to-the-bipartisan-us-house-ai-task-force-report/; Maria Curi, "What We're Hearing: Speaker Johnson on AI," Axios, May 2, 2024, https://www.axios.com/pro/tech-policy/2024/05/02/speaker-johnson-on-ai; Gopal Ratnam, "Schumer's AI Road Map Might Take GOP Detour," *Roll Call*, November 13, 2024, https://rollcall.com/2024/11/13/schumers-ai-road-map-might-take-gop-detour/.

15 Amber C. Thompson, et al., "Senate AI Working Group Releases Roadmap for Artificial Intelligence Policy," Mayer Brown, May 17, 2024, https://www.mayerbrown.com/en/insights/publications/2024/05/senate-ai-working-group-releases-roadmap-for-artificial-intelligence-policy.

16 "National Defense Authorization Act for Fiscal Year 2024," US Congress, 2023, https://www.congress.gov/bill/118th-congress/house-bill/2670.

17 "Summary of the Fiscal Year 2024 National Defense Authorization Act FY 2024," US Senate Committee on Armed Services, 2023, https://www.armed-services.senate.gov/imo/media/doc/fy24_ndaa_conference_executive_summary1.pdf. It is possible that the 2025 NDAA could be used to progress new AI legislation.

18 "Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence," White House, October 24, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/.

19 Provisions relating to especially sensitive national security issues, such as countermeasures for adversarial use of AI, are reserved to a classified annex.

20 Examples of self-imposed regulation include: "DOD Adopts Ethical Principles for Artificial Intelligence," US Department of Defense, February 24, 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/; Joseph Clark, "DOD Releases AI Adoption Strategy," US Department of Defense, November 2, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy; "DOD Directive 3000.09 Autonomy in Weapon Systems," US Department of Defense, January 25, 2023, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf; "Artificial Intelligence Ethics Framework for the Intelligence Community," Office of the Director of National Intelligence, June 2020, https://www.intelligence.gov/artificial-intelligence-ethics-framework-for-the-intelligence-community; "Principles of Artificial Intelligence Ethics for the Intelligence Community," Office of the Director of National Intelligence, June 2020, https://www.intelligence.gov/principles-of-artificial-intelligence-ethics-for-the-intelligence-community. For full analysis of the AI NSM, see: Gregory C. Allen and Isaac Goldston, "The Biden Administration's National Security Memorandum on AI Explained," Center for Strategic and International Studies, October 25, 2024, https://www.csis.org/analysis/biden-administrations-national-security-memorandum-ai-explained.

21 Ibid.

22 "Framework to Advance AI Governance and Risk Management in National Security," White House, October 24, 2024, https://ai.gov/wp-content/uploads/2024/10/NSM-Framework-to-Advance-AI-Governance-and-Risk-Management-in-National-Security.pdf.

ing of AI capabilities, saying, "preventing misuse and ensuring high standards of accountability will not slow us down; it will actually do the opposite."[23] An efficiency-based argument is likelier with a Trump administration focused on accelerating AI adoption.

4.1.3 State-level regulation

According to the National Conference of State Legislators, forty-five states introduced AI bills in 2024, and thirty-one adopted resolutions or enacted legislation.[24] These measures tend to focus on consumer rights and data privacy, but with significantly different approaches seen in the three states with the most advanced legislation: California, Utah, and Colorado.[25]

Having previously been a leader in data privacy legislation, the California State Legislature in 2024 passed what would have been the most far-reaching AI bill in the country before it was vetoed by Governor Gavin Newsom.[26] The bill had drawn criticism for potentially imposing arduous, and damaging, barriers to technological development in exactly the place where most US AI is developed.[27] However, Newsom supported a host of other AI-related bills in 2024 that will place significant restrictions and safeguards around the use of AI in California, indicating that the country's largest internal market will remain a significant force in the domestic regulation of AI.[28]

Colorado and Utah both successfully enacted AI legislation in 2024. Though both are consumer rights protection measures at their core, they take very different approaches. The Utah bill is quite narrowly focused on transparency and consumer protection around the use of generative AI, primarily through disclosure requirements placed on developers and deployers of AI services.[29] The Colorado bill is more broadly aimed at developers and deployers of "high-risk" AI systems, which here means an AI system that is a substantial factor in making any decision that can significantly impact an individual's legal or economic interests, such as decisions related to employment, housing, credit, and insurance.[30] This essentially gives Colorado a separate anti-discriminatory framework just for AI systems, which imposes reporting, disclosure, and testing obligations with civil penalties for violation.[31] This puts Colorado, not California, at the leading edge of state-level AI regulation, but that does not necessarily mean that other states will take the Colorado approach as precedent. In signing the law, Governor Jared Polis made clear that he had reservations, and a similar law was vetoed in Connecticut.[32] Some states might not progress restrictive AI regulation at all. For example, Virginia Governor Glenn Youngkin recently issued an executive order aiming to increase the use of AI in state government agencies, law enforcement, and education, but there is no indication that legislation will follow anytime soon.[33]

However state-level legislation progresses, it is unlikely to have any direct impact on military or national security users. There is also a risk that public fears around AI could be stoked and lead to more stringent state-level regulation, especially if AI is seen to "go wrong," leading to tangible examples of public harm. As discussed below in the context of the European

23 "Remarks by APNSA Jake Sullivan on AI and National Security," White House, October 25, 2024, https://www.whitehouse.gov/briefing-room/speeches-remarks/2024/10/24/remarks-by-apnsa-jake-sullivan-on-ai-and-national-security.

24 "Artificial Intelligence 2024 Legislation," National Conference of State Legislators, June 3, 2024, https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation.

25 Brian Joseph, "Common Themes Emerge in State AI Legislation," *Capitol Journal*, April 16, 2024, https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/common-themes-emerge-in-state-ai-legislation; John J. Rolecki, "Emerging Trends in AI Governance: Insights from State-Level Regulations Enacted in 2024," *National Law Review*, January 6, 2025, https://natlawreview.com/article/emerging-trends-ai-governance-insights-state-level-regulations-enacted-2024.

26 Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, SB-1047 (2024), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB1047.

27 Hodan Omaar, "California's Bill to Regulate Frontier AI Models Undercuts More Sensible Federal Efforts," Center for Data Innovation, February 20, 2024, https://datainnovation.org/2024/02/californias-bill-to-regulate-frontier-ai-models-undercuts-more-sensible-federal-efforts; Bobby Allyn, "California Gov. Newsom Vetoes AI Safety Bill That Divided Silicon Valley," NPR, September 29, 2024, https://www.npr.org/2024/09/20/nx-s1-5119792/newsom-ai-bill-california-sb1047-tech.

28 Hope Anderson, Nick Reem, and Sara Tadayyon, "Raft of California AI Legislation Adds to Growing Patchwork of US Regulation," White & Case, October 10, 2024, https://www.whitecase.com/insight-alert/raft-california-ai-legislation-adds-growing-patchwork-us-regulation; Myriah V. Jaworski and Ali Bloom, "A View from California: One Important Artificial Intelligence Bill Down, 17 Others Good to Go," Clark Hill, November 5, 2024, https://www.clarkhill.com/news-events/news/a-view-from-california-one-important-artificial-intelligence-bill-down-17-others-good-to-go.

29 Scott Young and Jordan Hilton, "Utah Enacts AI-Focused Consumer Protection Bill," Mayer Brown, May 13, 2024, https://www.mayerbrown.com/en/insights/publications/2024/05/utah-enacts-ai-focused-consumer-protection-bill.

30 "Colorado Enacts Groundbreaking Artificial Intelligence Act," Troutman Pepper Locke, May 29, 2024, https://www.regulatoryoversight.com/2024/05/colorado-enacts-groundbreaking-artificial-intelligence-act.

31 Jake Parker, "Misgivings Cloud First-In-Nation Colorado AI Law: Implications and Considerations for the Security Industry," Security Industry Association, May 28, 2024, https://www.securityindustry.org/2024/05/28/misgivings-cloud-first-in-nation-colorado-ai-law-implications-and-considerations-for-the-security-industry.

32 Bente Birkeland, "In Writing the Country's Most Sweeping AI Law, Colorado Focused on Fairness, Preventing Bias," NPR, June 22, 2024, https://www.npr.org/2024/06/22/nx-s1-4996582/artificial-intelligence-law-against-discrimination-hiring-colorado.

33 Daniel Castro, "Virginia's New AI Executive Order Is a Model for Other States to Build On," Center for Data Innovation, February 16, 2024, https://datainnovation.org/2024/02/virginias-new-ai-executive-order-is-a-model-for-other-states-to-build-on.

US President Joe Biden hosts a meeting on artificial intelligence in June 2023 at the Fairmont Hotel in San Francisco, California alongside Sal Khan, Arati Prabhakar, California Governor Gavin Newsom, and Joy Buolamwini. Source: White House

Union, the use of AI in law enforcement is among the most controversial use cases. This can only be more relevant in the nation with some of the most militarized police forces in the world and a National Guard that can also serve a domestic law-enforcement role.[34]

4.1.4 International efforts

The United States has been active in a number of international initiatives relating to AI regulation, including through the UN, NATO, and the G7 Hiroshima process, which are covered later in this paper. The final element of the Biden administration's approach to AI regulation, and the one that might be the least likely to carry through into 2025, was the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy.[35] The declaration is a set of non-legally binding guidelines that aims to promote responsible behavior and demonstrate US leadership in the international arena. International norms are notoriously hard to agree upon and even harder to enforce. Unsurprisingly, the declaration makes no effort to restrict the kinds of AI systems that signatories can develop in their pursuit of national defense. According to the DoD, forty-seven nations have endorsed the declaration, though China, Russia, and Iran are notably not among that number.[36]

34 "War Comes Home: The Excessive Militarization of American Police," American Civil Liberties Union, June 23, 2014, https://www.aclu.org/publications/war-comes-home-excessive-militarization-american-police; Anshu Siripurapu and Noah Berman, "What Does the U.S. National Guard Do?" Council on Foreign Relations, April 3, 2024, https://www.cfr.org/backgrounder/what-does-us-national-guard-do.

35 "Fact Sheet: The Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy," US Department of State, November 27, 2024, https://www.state.gov/political-declaration-on-the-responsible-military-use-of-artificial-intelligence-and-autonomy.

36 Brandi Vincent, "US Eyes First Multinational Meeting to Implement New 'Responsible AI' Declaration," DefenseScoop, January 9, 2024, https://defensescoop.com/2024/01/09/us-eyes-first-multinational-meeting-to-implement-new-responsible-ai-declaration.

4.2 China

The Chinese approach to AI regulation is relatively straightforward compared to that of the United States, with rules issued in a top-down, center-outward manner in keeping with the general mode of Chinese government.

4.2.1 Overview

Regulatory approach

China has a vertical, technology-driven approach with some horizontal, use-case, and sectoral elements.

It is focused on general-purpose AI, with some additional regulation for specific use cases.

Scope of regulation

The primary unit of regulation is AI algorithms, with specific restrictions on the use of training data in some cases.

Type of regulation

China uses hard regulation with a strong compliance regime and significant room for politically interested interpretation in enforcement.

Target of regulation

Regulation is narrowly targeted to privately owned service providers operating AI systems within China and those entities providing AI-enabled services to the Chinese population.

Coverage of defense and national security

These areas are not covered and unlikely to be covered in the future.

4.2.2 Domestic regulation

Since 2018, the Chinese government has issued four administrative provisions intended to regulate delivery of AI capabilities to the Chinese public, most notably the so-called Generative AI Regulation, which came into force in August 2023.[37] This, and preceding provisions on the use of algorithmic recommendations in service provision and the more general use of deep synthesis tools, is focused on regulating algorithms rather than specific use cases.[38] This vertical approach to regulation is also iterative, allowing Chinese regulators to build skills and toolsets that can adapt as the technology develops. A more comprehensive AI law is expected at some point but, at the time of writing, only a scholars' draft released by the Chinese Academy of Social Sciences (CASS) gives outside observers insight into how the Chinese government is thinking about future AI regulation.[39]

The draft proposes the formation of a new government agency to coordinate and oversee AI in public services. Importantly, and unlike in the United States, the use of AI by the Chinese government itself is not covered by any proposed or existing regulations, including for military and other national security purposes. This approach will likely not change, as it serves the Chinese government's primary goal, which is to preserve its central control over the flow of information to maintain internal political and social stability.[40] The primary regulatory tool proposed by the scholars' draft is a reporting and licensing regime in which items that appear on a negative list would require a government-approved permit for development and deployment. This approach is a way for the Chinese government to manage safety and other risks while still encouraging innovation.[41] The draft is not clear about what items would be on the list, but foundational models are explicitly referenced. In addition to an emerging licensing regime and ideas about the role of a bespoke regulator, Chinese regulations have reached interim conclusions in areas in which the United States and others are still in debate. For example, the Generative AI Regulation explicitly places liability for AI systems on the service providers that make them available to the Chinese public.[42]

Enforcement is another area in which the Chinese government is signaling a different approach. As one commentator notes, "Chinese regulation is stocked with provisions that are straight off the wish list for AI to support supposed democratic values [. . .] yet the regulation is clearly intended to strengthen China's

37 "How Does China's Approach to AI Regulation Differ from the US and EU?" Forbes, July 18, 2023, https://www.forbes.com/sites/forbeseq/2023/07/18/how-does-chinas-approach-to-ai-regulation-differ-from-the-us-and-eu/?sh=47763973351c.

38 Matt Sheehan, "China's AI Regulations and How They Get Made," Carnegie Endowment for International Peace, July 10, 2023, https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en.

39 CASS is an official Chinese think tank operating under the State Council. "China's New AI Regulations," Latham & Watkins Privacy & Cyber Practice, August 16, 2023, https://www.lw.com/admin/upload/SiteAttachments/Chinas-New-AI-Regulations.pdf; Zac Haluza, "How Will China's Generative AI Regulations Shape the Future?" DigiChina Forum, April 26, 2023, https://digichina.stanford.edu/work/how-will-chinas-generative-ai-regulations-shape-the-future-a-digichina-forum; Zeyi Yang, "Four Things to Know about China's New AI Rules in 2024," *MIT Technology Review*, January 17, 2024, https://www.technologyreview.com/2024/01/17/1086704/china-ai-regulation-changes-2024.

40 Sheehan, "China's AI Regulations and How They Get Made."

41 Graham Webster, et al., "Analyzing an Expert Proposal for China's Artificial Intelligence Law," DigiChina, Stanford University, August 29, 2023, https://digichina.stanford.edu/work/forum-analyzing-an-expert-proposal-for-chinas-artificial-intelligence-law.

42 Mark MacCarthy, "The US and Its Allies Should Engage with China on AI Law and Policy," Brookings, October 19, 2023, https://www.brookings.edu/articles/the-us-and-its-allies-should-engage-with-china-on-ai-law-and-policy.

authoritarian system of government."[43] Analysis from the East Asia Forum suggests that China is continuing to refine how it balances innovation and control in its approach to AI governance.[44] If this is true, then the vague language in Chinese AI regulations, which would give Chinese regulators huge freedom in where and how they make enforcement decisions, could be precisely the point.[45]

4.2.3 International efforts

As noted above, China has not endorsed the United States' Political Declaration on the Responsible Military Use of Artificial Intelligence and Autonomy, but China is active on the international AI stage in other ways. At a 2018 meeting relating to the United Nations Convention on Certain Conventional Weapons, the Chinese representative presented a position paper proposing a ban on lethal autonomous weapons (LAWS).[46] But Western observers doubt the motives behind the proposal, with one commentator saying it included "such a bizarrely narrow definition of lethal autonomous weapons that such a ban would appear to be both unnecessary and useless."[47] China has continued calling for a ban on LAWS in UN forums and other public spaces, but these calls are usually seen in the West as efforts to appear as a positive international actor while maintaining a position of strategic ambiguity—there is little faith that the Chinese government will practice what it preaches.[48] This is most clearly seen in reactions to the Global Security Initiative (GSI) concept paper published in February 2023.[49] Reacting to this proposal, which China presented as aspiring for a new and more inclusive global security architecture, the US-China Economic and Security Review Commission (USCC) responded with scorn, saying, "the GSI's core objective appears to be the degradation of U.S.-led alliances and partnerships under the guise of a set of principles full of platitudes but empty on substantive steps for contributing to global peace."[50]

Outside of the military sphere, Chinese involvement in international forums attracts similar critique. In the lead-up to the United Kingdom's AI Safety Summit, the question of whether China would be invited, and then whether Beijing's representatives would attend, caused controversy and criticism.[51] However, that Beijing is willing to collaborate internationally in areas where it sees benefit does not mean that Beijing will toe the Western line. In fact, Western-led international regulation might not even be a particular concern for China. Shortly after the AI Safety Summit, Chinese President Xi Jinping announced a new Global AI Governance Initiative.[52] As with the GSI, this effort has been met with skepticism in the United States, but there is a real risk that China's approach could split international regulation into two spheres.[53] This risk is especially salient because of the initiative's potential appeal to the Global South. More concerningly, there is some evidence that China is pursuing a so-called proliferation-first approach, which involves pushing its AI technology into developing countries. If China manages to embed itself in the global AI infrastructure in the way that it did with fifth-generation (5G) technology, then any attempt to regulate international standards might come too late—those standards will already be Chinese.[54]

---

43 Matt O'Shaughnessy, "What a Chinese Regulation Proposal Reveals about AI and Democratic Values," Carnegie Endowment for International Peace, May 16, 2023, https://carnegieendowment.org/posts/2023/05/what-a-chinese-regulation-proposal-reveals-about-ai-and-democratic-values?lang=en.

44 Huw Roberts and Emmie Hine, "The Future of AI Policy in China," *East Asia Journal*, September 27, 2023, https://eastasiaforum.org/2023/09/27/the-future-of-ai-policy-in-china/.

45 Will Henshall, "How China's New AI Rules Could Affect U.S. Companies," *Time*, September 19, 2023, https://time.com/6314790/china-ai-regulation-us.

46 "CCW/GGE.1/2018/WP.7 Position Paper: Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects," China in Delegation to UN-CCW, April 11, 2018, https://unoda-documents-library.s3.amazonaws.com/Convention_on_Certain_Conventional_Weapons_-_Group_of_Governmental_Experts_(2018)/CCW_GGE.1_2018_WP.7.pdf.

47 Gregory C. Allen, "Understanding China's AI Strategy," Center for a New American Security, February 6, 2019, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

48 Putu Shangrina Pramudia, "China's Strategic Ambiguity on the Issue of Autonomous Weapons Systems," *Global: Jurnal Politik Internasional* 24, 1 (2022), https://scholarhub.ui.ac.id/global/vol24/iss1/1/; Gregory C. Allen, "One Key Challenge for Diplomacy on AI: China's Military Does Not Want to Talk," Center for Strategic and International Studies, May 20, 2022, https://www.csis.org/analysis/one-key-challenge-diplomacy-ai-chinas-military-does-not-want-talk.

49 "Full Text: The Global Security Initiative Concept Paper," Embassy of the People's Republic of China, 2023, http://cr.china-embassy.gov.cn/esp/ndle/202302/t20230222_11029046.htm.

50 Sierra Janik, et al., "China's Paper on Ukraine and next Steps for Xi's Global Security Initiative," US-China Economic and Security Review Commission, July 17, 2024, https://www.uscc.gov/research/chinas-paper-ukraine-and-next-steps-xis-global-security-initiative.

51 Joyce Hakmeh, "Balancing China's Role in the UK's AI Agenda," Chatham House, October 30, 2023, https://www.chathamhouse.org/2023/10/balancing-chinas-role-uks-ai-agenda.

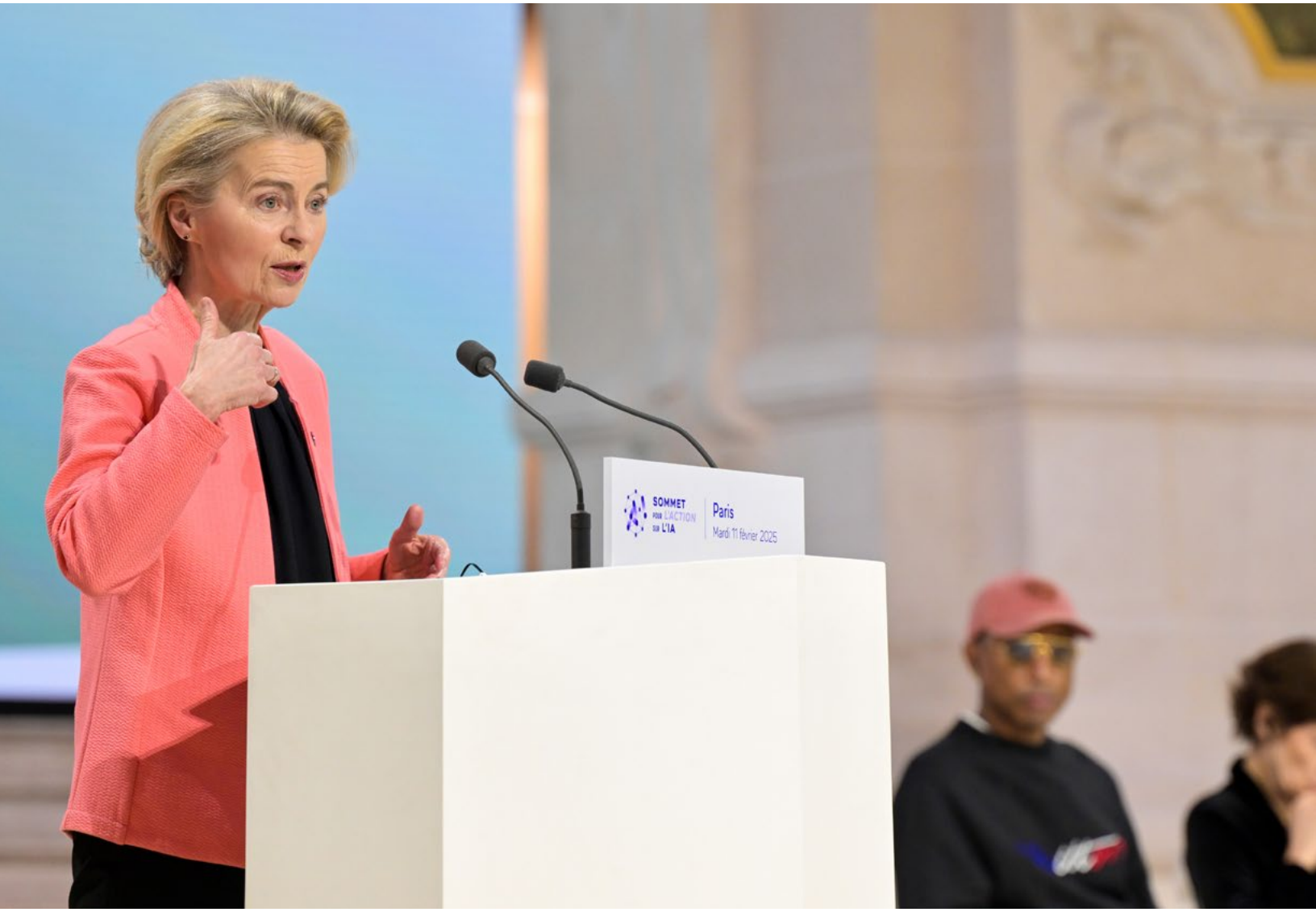
52 "Global AI Governance Initiative," Embassy of the People's Republic of China, 2023, http://gd.china-embassy.gov.cn/eng/zxhd_1/202310/t20231024_11167412.htm.

53 Shannon Tiezzi, "China Renews Its Pitch on AI Governance at World Internet Conference," Diplomat, November 9, 2023, https://thediplomat.com/2023/11/china-renews-its-pitch-on-ai-governance-at-world-internet-conference.

54 Bill Drexel and Hannah Kelley, "Behind China's Plans to Build AI for the World," *Politico*, November 30, 2023, https://www.politico.com/news/magazine/2023/11/30/china-global-ai-plans-00129160.

4.3 European Union

The European Union moved early into the AI regulation game. In August 2024, it became the first legislative body globally to issue legally binding rules around the development, deployment, and use of AI.[55] Originally envisaged as a consumer protection law, early drafts of the AI Act covered AI systems only as they are used in certain narrowly limited tasks—a horizontal approach.[56] However, the explosion of interest in foundational models following the release of ChatGPT in late 2022 led to an expansion in the law's scope to include these kinds of models regardless of how and by whom they are used.



In February 2025, Ursula von der Leyen, President of the European Commission, participated in the Artificial Intelligence Action Summit in Paris, France. Source: Dati Bendo/European Union, 2025/EC - Audiovisual Service

55 "AI Act Enters into Force," European Commission, August 1, 2024, https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en.

56 The AI Act is formally called the Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Legislative Acts.

4.3.1 Overview

Regulatory approach

The approach is horizontal, with a vertical element for general-purpose AI systems.

Specific use cases are based on risk assessment.

Scope of regulation

The scope is widest for high-risk and general-purpose AI systems. This includes data, algorithms, applications, and content provenance.

Hardware is not covered, but general-purpose AI system elements use a compute-power threshold definition.

Type of regulation

The EU uses hard regulation with high financial penalties for noncompliance.

A full compliance and enforcement regime is still in development but will incorporate the EU AI Office and member states's institutions.

Target of regulation

The regulation targets AI developers, with more limited responsibilities placed on deployers of high-risk systems.

Coverage of defense and national security

Defense is specifically excluded on institutional competence grounds, but domestic policing use cases are covered, with some falling into the unacceptable and high-risk groups.

4.3.2 Internal regulation

The AI Act is an EU regulation, the strongest form of legislation that the EU can produce, and is binding and directly applicable in all member states.[57] The AI Act takes a risk-based approach whereby AI systems are regulated by how they are used, based on the potential harm that use could cause to an EU citizen's health, safety, and fundamental rights. There are four categories of risk: unacceptable, high, limited, and minimal/none. Systems in the limited and minimal categories are subject to obligations around attribution and informed consent, i.e., people must know they are talking to a chatbot or viewing an AI-generated image. At the other end of the scale, AI systems that fall within the unacceptable risk category are completely prohibited. This includes any AI system used for social scoring, unsupervised criminal profiling, or workplace monitoring; systems that exploit vulnerabilities or impair a person's ability to make informed decisions via manipulation; biometric categorization of sensitive characteristics; untargeted use of facial recognition; and the use of real-time remote biometric identification systems in public spaces, except for narrowly defined police use cases.[58]

High-risk systems are subject to the most significant regulation in the AI Act and are defined as such by two mechanisms. First, AI systems used as a safety component or within a kind of product already subject to EU safety standards are automatically high risk.[59] Second, AI systems are considered high risk if they are used in the following areas: biometrics; critical infrastructure; education and vocational training; employment, worker management, and access to self-employment; access to essential services; law enforcement; migration, asylum, and border-control management; and administration of justice and democratic processes.[60] The majority of obligations fall on developers of high-risk AI systems, with fewer obligations placed on deployers of those systems.[61]

As mentioned, so-called general-purpose AI (GPAI) is covered separately in the AI Act. This addition was a significant bone of contention in the trilogue negotiation, as some member states were concerned that vertical regulation of specific kinds of AI

57 Hadrien Pouget, "Institutional Context: EU Artificial Intelligence Act," EU Artificial Intelligence Act, 2019, https://artificialintelligenceact.eu/context.

58 "Chapter 2, Article 5—Prohibited AI Practices in Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance)," EUR-Lex, European Union, 2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

59 This covers a huge swath of consumer devices including toys, medical devices, motor vehicles, and gas-burning appliances.

60 "Chapter 3, Section 1, Article 5—Classification Rules for High-Risk AI Systems in Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance)," EUR-Lex, European Union, 2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

61 Developers of high-risk AI systems must implement comprehensive risk-management and data-governance practices throughout the life cycle of the system; meet standards for accuracy, robustness, and cybersecurity; and register the system in an EU-wide public database. Mia Hoffmann, "The EU AI Act: A Primer," Center for Security and Emerging Technology, Georgetown University, September 26, 2023, https://cset.georgetown.edu/article/the-eu-ai-act-a-primer.

would stifle innovation in the EU.[62] As a compromise, though all developers of GPAI must provide technical documentation and instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training, the more stringent obligations akin to those imposed on developers of high-risk systems are reserved for GPAI models that pose "systemic risk."[63] Open-license developers must comply with these restrictions only if their models fall into this last category.[64]

It is not yet clear exactly how the new European AI Office will coordinate compliance, implementation, and enforcement. As with all new EU regulation, interpretation through national and EU courts will be critical.[65] One startling feature of the AI Act is the leeway it appears to give the technology industry by allowing developers to self-determine their AI system's risk category, though the huge financial penalties those who violate the act face might serve as sufficient deterrent to bad actors.[66]

The AI Act does not, and could never, apply directly to military or defense applications of AI because the European Union does not have authority in these areas. As expected, the text includes a general exemption for military, defense, and national security uses, but exemptions for law enforcement are far more complicated and were some of the most controversial sections in final negotiations.[67] Loopholes allowing police to use AI in criminal profiling, if it is part of a larger, human-led toolkit, and the use of AI facial recognition on previously recorded video footage have caused uproar and seem likely candidates for litigation, potentially placing increased costs and uncertainty on developers working in these areas.[68] This ambiguity could have knock-on effects, given the increasing overlap between military technologies and those used by police and other national security actors, especially in counterterrorism.

4.3.3 International efforts

The official purpose of the AI Act is to set consistent standards across member states in order to ensure that the single market can function effectively, but some believe that this will lead the EU to effectively become the world's AI police.[69] Part of this is the simple fact that it will be a lot easier for other jurisdictions to copy and paste a regulatory model that has already been proven, but concern comes from the way that the General Data Protection Regulation (GDPR) has had huge influence outside of the territorial boundaries of the EU by placing a high cost of compliance on companies that want to do business in or with the world's second-largest economic market.[70] Similarly, EU regulations on the kinds of charging ports that can be used for small electronic devices have resulted in changes well beyond its borders.[71] However, more recently, Apple has decided to hold back on releasing AI features to users in the EU, indicating that cross-border influence can run both ways.[72]

62 Jedidiah Bracy, "EU AI Act: Draft Consolidated Text Leaked Online," International Association of Privacy Professionals, January 22, 2024, https://iapp.org/news/a/eu-ai-act-draft-consolidated-text-leaked-online.

63 "Chapter 5, Section 1, Article 51—Classification of General-Purpose AI Models as General-Purpose AI Models with Systemic Risk and Article 52—Procedure in Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance)," EUR-Lex, European Union, 2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

64 Lisa Peets, Marianna Drake, and Marty Hansen, "EU AI Act: Key Takeaways from the Compromise Text," Inside Privacy, February 28, 2024, https://www.insideprivacy.com/artificial-intelligence/eu-ai-act-key-takeaways-from-the-compromise-text.

65 Hadrien Pouget and Johann Laux, "A Letter to the EU's Future AI Office," Carnegie Endowment for International Peace, 2023, https://carnegieendowment.org/2023/10/03/letter-to-eu-s-future-ai-office-pub-90683.

66 Hoffman, "The EU AI Act: A Primer"; Osman Gazi Güçlütürk, Siddhant Chatterjee, and Airlie Hilliard, "Penalties of the EU AI Act: The High Cost of Non-Compliance," Holistic AI, February 18, 2024, https://www.holisticai.com/blog/penalties-of-the-eu-ai-act.

67 Jedidah Bracy and Alex LaCasse, "EU Reaches Deal on World's First Comprehensive AI Regulation," International Association of Privacy Professionals, December 11, 2023, https://iapp.org/news/a/eu-reaches-deal-on-worlds-first-comprehensive-ai-regulation.

68 Gian Volpicelli, "EU Set to Allow Draconian Use of Facial Recognition Tech, Say Lawmakers," *Politico*, January 16, 2024, https://www.politico.eu/article/eu-ai-facial-recognition-tech-act-late-tweaks-attack-civil-rights-key-lawmaker-hahn-warns.

69 Melissa Heikkilä, "Five Things You Need to Know about the EU's New AI Act," *MIT Technology Review*, December 11, 2023, https://www.technologyreview.com/2023/12/11/1084942/five-things-you-need-to-know-about-the-eus-new-ai-act.

70 Jennifer Wu and Martin Hayward, "International Impact of the GDPR Felt Five Years On," Pinsent Masons, June 6, 2023, https://www.pinsentmasons.com/out-law/analysis/international-impact-of-the-gdpr-felt-five-years-on.

71 Kevin Purdy, "USB-C Is Now the Law of the Land in Europe," *Wired*, January 3, 2025, https://www.wired.com/story/usb-c-is-now-a-legal-requirement-for-most-rechargeable-gadgets-in-europe.

72 Apple has said that this decision isn't related to the AI Act, but rather the earlier Digital Markets Act (DMA), which aims to prevent large companies from abusing their market power with massive fines of up to 10 percent of the company's total worldwide annual turnover, or up to 20 percent in the event of repeated infringements. "Apple's AI Has Now Been Released but It's Not Coming to Europe," Euronews and Associated Press, October 29, 2024, https://www.euronews.com/next/2024/10/29/apples-ai-has-now-been-released-but-its-not-coming-to-europe-any-time-soon.

4.4 United Kingdom

Since 2022, the UK government has described its approach to AI regulation as innovation-friendly and flexible, designed to service the potentially contradictory goals of encouraging economic growth through innovation while also safeguarding fundamental values and the safety of the British public.[73] This approach was developed under successive Conservative governments but is yet to change radically under the Labour government as it attempts to balance tensions between business-friendly elements of the party and more traditional labor activists and trade unionists.[74]

4.4.1 Overview

Regulatory approach

The approach is horizontal and sectoral for now, with some vertical elements possible for general-purpose AI systems.

Scope of regulation

The scope is unclear. Guidance to regulators refers primarily to AI systems with some consideration of supply chain components. It will likely vary by sector.

Type of regulation

There is hard regulation through existing sectoral regulators and their compliance and enforcement regimes, with the possibility of more comprehensive hard regulation in the future.

Target of regulation

The target varies by sector. Guidance to existing regulators generally focuses on AI developers and deployers.

Coverage of defense and national security

Bespoke military and national security frameworks sit alongside a broader government framework.

4.4.2 Domestic regulation

The UK's approach to AI regulation was first laid out in June 2022, followed swiftly by a National AI Strategy that December and a subsequent policy paper in August 2023, which set out the mechanisms and structures of the regulatory approach in more detail.[75] However, this flurry of policy publications has not resulted in any new laws.[76] During the 2024 general election campaign, members of the new Labour government initially promised to toughen AI regulation, including by forcing AI companies to release test data and conduct safety tests with independent oversight, before taking a more conciliatory tone with the technology industry and promising to speed up the regulatory process to encourage innovation.[77] Though its legislative agenda initially included appropriate legislation for AI by the end of 2024, this has not been realized.[78] The prevailing view seems to be that, with some specific exceptions, existing regulators are best placed to understand the needs and peculiarities of their sectors.[79]

73 Paul Shepley and Matthew Gill, "Artificial Intelligence: How Is the Government Approaching Regulation?" Institute for Government, October 27, 2023, https://www.instituteforgovernment.org.uk/explainer/artificial-intelligence-regulation.

74 Vincent Manancourt, Tom Bristow, and Laurie Clarke, "Friend or Foe: Labour's Looming Battle on AI," *Politico*, October 12, 2023, https://www.politico.eu/article/friend-or-foe-labour-party-keir-starmer-looming-battle-ai-artificial-intelligence.

75 "Establishing a Pro-Innovation Approach to Regulating AI," UK Government, July 18, 2022, https://www.gov.uk/government/publications/establishing-a-pro-innovation-approach-to-regulating-ai/establishing-a-pro-innovation-approach-to-regulating-ai-policy-statement; "National AI Strategy," Government of the United Kingdom, September 22, 2021, https://www.gov.uk/government/publications/national-ai-strategy; "A Pro-Innovation Approach to AI Regulation," Government of the United Kingdom, March 22, 2023, https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#executive-summary.

76 This decision is likely, in part, a result of political pragmatism (legislation takes time and parliamentary time is limited) but it also reflects the nature of the United Kingdom's parliamentary system, which allows the government of the day significant leeway in interpretation of primary legislation, including through secondary legislation and various kinds of subordinate regulatory instruments that may be delegated to public bodies. "Understanding Legislation," Parliament of the United Kingdom, 2018, https://www.legislation.gov.uk/understanding-legislation.

77 Tom Bristow, "Labour Will Toughen up AI Regulation, Starmer Says," Politico, June 13, 2023, https://www.politico.eu/article/starmer-labour-will-bring-in-stronger-ai-regulation; Dan Milmo, "Labour Would Force AI Firms to Share Their Technology's Test Data," *Guardian*, February 4, 2024, https://www.theguardian.com/technology/2024/feb/04/labour-force-ai-firms-share-technology-test-data.

78 "King's Speech," Hansard, UK Parliament, July 17, 2024, https://hansard.parliament.uk/Commons/2024-07-17/debates/2D7D3E47-776E-4B81-8E2A-7854168D6FED/King%E2%80%99SSpeech; Anna Gross and George Parker, "UK's AI Bill to Focus on ChatGPT-Style Models," *Financial Times*, August 1, 2024, https://www.ft.com/content/ce53d233-073e-4b95-8579-e80d960377a4.

79 "A Pro-Innovation Approach to AI Regulation."

Some regulators are already taking steps to incorporate AI into their frameworks. The Financial Conduct Authority's Regulatory Sandbox allows companies to test AI-enabled products and services in a controlled environment and, by doing so, to identify consumer protection safeguards that might be necessary.[80] The Digital Regulation Cooperation Forum (DRCF) recently launched its AI and Digital Hub, a twelve-month pilot program to make it easier for companies to launch new AI products and services in a safe and compliant manner, and to reduce the time it takes to bring those products and services to market.[81]

Though the overall approach is sectoral, there is some central authority in the UK approach. The Office for AI has no regulatory role but is expected to provide certain central functions required to monitor and evaluate the effectiveness of the regulatory framework.[82] Another centrally run AI authority, the AI Safety Institute (AISI), breaks from the sectoral approach and instead focuses on "advanced AI," which includes GPAI systems as well as narrow AI models that have the potential to cause harm in specific use cases.[83] While AISI is not a regulator, several large technology companies, including OpenAI, Google, and Microsoft, have signed voluntary agreements to allow AISI to test these firms' most advanced AI models and make changes to them if they find safety concerns.[84] However, now that AISI has found significant flaws in those same models, both AISI and the companies have stepped back from that position, demonstrating the inherent limitations of voluntary regimes. In recognition of this dilemma, the forthcoming legislation referenced above is expected to make existing voluntary agreements between companies and the government legally binding.[85]

The most significant challenge to the current sector-based approach is likely to come from the UK Competition and Markets Authority (CMA). Having previously taken the view that flexible guiding principles would be sufficient to preserve competition and consumer protection, the CMA is now concerned that a small number of technology companies increasingly have the ability and incentive to engage in market-distorting behavior in their own interests.[86] The CMA has also proposed prioritizing GPAI under new regulatory powers provided by the Digital Markets, Competition and Consumers Bill (DMCC).[87] A decision to do so could have a huge impact on the AI industry, as the DMCC significantly sharpens the CMA's teeth, giving it the power to impose fines for violation of up to 10 percent of global turnover without involvement of a judge, as well as smaller fines for senior individuals within corporate entities and consumer compensation.[88]

As in the United States, it is expected that any UK legislative or statutory effort to expand the regulatory power of government over AI will have some kind of exemption for national security usage.[89] But, as in the United States, it does not follow that the national security community will be untouched by regulation. The UK Ministry of Defence (UK MOD) published its own AI strategy in June 2022, accompanied by a policy statement

80 "Regulatory Sandbox," Financial Conduct Authority, August 1, 2023, https://www.fca.org.uk/firms/innovation/regulatory-sandbox.

81 DRCF brings together the four UK regulators with responsibilities for digital regulation—the Competition and Markets Authority (CMA), the Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO), and Ofcom—to collaborate on digital regulatory matters. "The DRCF Launches Informal Advice Service to Support Innovation and Enable Economic Growth," Digital Regulation Cooperation Forum, April 22, 2024, https://www.drcf.org.uk/publications/press-releases/the-drcf-launches-informal-advice-service-to-support-innovation-and-enable-economic-growth.

82 This includes through implementation guidelines, 10 million pounds of funding to boost regulators' capabilities in AI, and ensuring interoperability with international regulatory frameworks. "Implementing the UK's AI Regulatory Principles Initial Guidance for Regulators," Government of the United Kingdom, February 2024, https://www.gov.uk/government/publications/implementing-the-uks-ai-regulatory-principles-initial-guidance-for-regulators.

83 "Introducing the AI Safety Institute," Government of the United Kingdom, last updated January 17, 2024, https://www.gov.uk/government/publications/ai-safety-institute-overview/introducing-the-ai-safety-institute; "AI Safety Institute Approach to Evaluations," Government of the United Kingdom, February 9, 2024, https://www.gov.uk/government/publications/ai-safety-institute-approach-to-evaluations/ai-safety-institute-approach-to-evaluations.

84 Madhumita Murgia, Anna Gross, and Cristina Criddle, "World's Biggest AI Tech Companies Push UK over Safety Tests," *Financial Times*, February 7, 2024, https://www.ft.com/content/105ef217-9cb2-4bd2-b843-823f79256a0e.

85 Dan Milmo, "AI Safeguards Can Easily Be Broken, UK Safety Institute Finds," *Guardian*, February 9, 2024, https://www.theguardian.com/technology/2024/feb/09/ai-safeguards-can-easily-be-broken-uk-safety-institute-finds; Gross and Parker, "UK's AI Bill to Focus on ChatGPT-Style Models."

86 "AI Foundation Models Review: Short Version," Competition and Markets Authority, September 18, 2023, https://assets.publishing.service.gov.uk/media/65045590dec5be000dc35f77/Short_Report_PDFA.pdf; Sarah Cardell, "Opening Remarks at the American Bar Association (ABA) Chair's Showcase on AI Foundation Models," Government of the United Kingdom, April 10, 2024, https://www.gov.uk/government/speeches/opening-remarks-at-the-american-bar-association-aba-chairs-showcase-on-ai-foundation-models. The CMA is known to be looking at Microsoft's partnership with OpenAI and has recently opened a "Phase 1" investigation into Amazon's recent $4-billion investment in Anthropic to assess whether the deal may harm competition. Ryan Browne, "Amazon's $4 Billion Investment in AI Firm Anthropic Faces UK Merger Investigation," CNBC, August 8, 2024, https://www.cnbc.com/2024/08/08/amazons-investment-in-ai-firm-anthropic-faces-uk-merger-investigation.html.

87 "AI Foundation Models Update Paper," Competition and Markets Authority, 2024 https://www.gov.uk/government/publications/ai-foundation-models-update-paper.

88 Meredith Broadbent, "UK Digital Markets, Competition and Consumers Bill: Extraterritorial Regulation Affecting the Tech Investment Climate," Center for Strategic and International Studies, March 4, 2024, https://www.csis.org/analysis/uk-digital-markets-competition-and-consumers-bill-extraterritorial-regulation-affecting.

89 "A Pro-Innovation Approach to AI Regulation."

on the ethical principles that the UK armed forces will follow in developing and deploying AI-enabled capabilities.[90] Both documents recognize that the use of AI in the military sphere comes with a specific set of risks and concerns that are potentially more acute than those in other sectors. These documents also stress that the use of any technology by the armed forces and their supporting organizations is already subject to a robust regime of compliance for safety, where the Defence Safety Agency has enforcement authorities; and legality, where existing obligations under UK and international human rights law and the law of armed conflict form an irreducible baseline.

The UK's intelligence community does not have a director of national intelligence to issue community-wide guidance on AI, but the Government Communications Headquarters (GCHQ) offers some insight into how the relevant agencies are thinking about the issue.[91] Published in 2021, GCHQ's paper on the Ethics of Artificial Intelligence predates the current regulatory discussion but slots neatly into the sectoral approach.[92] In the paper, GCHQ points to existing legislative provisions that ensure its work complies with the law. Most relevant for discussion of AI is the role of the Technology Advisory Panel (TAP), which sits within the Investigatory Powers Commissioner's Office and advises on the impact of new technologies in covert investigations.[93] The implicit argument underpinning both the UK MOD and GCHQ approaches is that specific regulations or restrictions on the use of AI in national security are needed only insofar as AI presents risks that are not captured by existing processes and procedures. Ethical principles, like the five to which the UK MOD will hold itself, are intended to frame and guide those risk assessments at all stages of the capability development and deployment process, but they are not in themselves regulatory.[94] As civil regulation of AI develops, it will be necessary to continue testing the assumption that the existing national security frameworks are capable of addressing AI risks and to change them as needed, including to ensure that they are sufficient to satisfy a supply base, international community, and public audience that might expect different standards.

4.4.3 International efforts

In addition to active participation in multilateral discussions through the UN, OECD, and the G7, the United Kingdom has held itself out to be a global leader in AI safety. The inaugural Global AI Safety Summit held in late 2023 delivered the Bletchley Declaration, a statement signed by twenty-eight countries in which they agreed to work together to ensure "human-centric, trustworthy and responsible AI that is safe" and to "promote cooperation to address the broad range of risks posed by AI."[95] The Bletchley Declaration has been criticized for its focus on the supposed existential risks of GPAI at the expense of more immediate safety concerns and for its lack of any specific rules or roadmap.[96] But it gives an indication of the areas of AI regulation in which it might be possible to find common ground, which, in turn, might limit the risk of entirely divergent regulatory regimes.[97]

90 "Defence Artificial Intelligence Strategy," Government of the United Kingdom, June 15, 2022, https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy; "Ambitious, Safe, Responsible: Our Approach to the Delivery of AI-Enabled Capability in Defence," Government of the United Kingdom, June 15, 2022, https://www.gov.uk/government/publications/ambitious-safe-responsible-our-approach-to-the-delivery-of-ai-enabled-capability-in-defence/ambitious-safe-responsible-our-approach-to-the-delivery-of-ai-enabled-capability-in-defence.

91 GCHQ is the UK's signal intelligence agency.

92 "Pioneering a New National Security: The Ethics of Artificial Intelligence at GCHQ," Government of the United Kingdom, February 24, 2021, https://www.gchq.gov.uk/artificial-intelligence/index.html.

93 "Technology Advisory Panel—IPCO," Investigatory Powers Commissioner, 2021, https://www.ipco.org.uk/who-we-are/technology-advisory-panel.

94 The five principles are: human centricity; responsibility; understanding; bias and harm mitigation; and reliability.

95 "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023," Government of the United Kingdom, November 1, 2023, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

96 Thomas Macaulay, "World-First AI Safety Deal Exposes Agenda Set in Silicon Valley, Critics Say," Next Web, November 2, 2023, https://thenextweb.com/news/ai-safety-summit-bletchley-declaration-concerns.

97 Sean Ó hÉigeartaigh, "Comment on the Bletchley Declaration," Centre for the Study of Existential Risk, University of Cambridge, November 1, 2024, https://www.cser.ac.uk/news/comment-bletchley-declaration/.

4.5 Singapore

With a strong digital economy and a global reputation as pro-business and pro-innovation, Singapore is unsurprisingly approaching AI regulation along the same middle path between encouraging growth and preventing harms as the United Kingdom.[98] Unlike the United Kingdom, Singapore has carefully maintained its position as a neutral player between the United States and China, and this positioning is reflected in its strategy documents and public statements.[99]

4.5.1 Overview

Regulatory approach

The approach is horizontal and sectoral for now, with a future vertical element for general-purpose AI systems.

Scope of regulation

The proposed Model AI Governance Framework for Generative AI includes data, algorithms, applications, and content provenance.

In practice, it will vary by sector.

Type of regulation

It is hard regulation through existing sectoral regulators and their compliance and enforcement regimes.

Target of regulation

The targets include developers, application deployers, and service providers/hosting platforms.

Responsibility is allocated based on the level of control and differentiated by the stage in the development and deployment cycle.

Coverage of defense and national security

No publicly available framework.

4.5.2 Domestic regulation

Government activity in the area is driven by the second National AI Strategy (NAIS 2.0), which is partly a response to the increasing concern over the safety and security of AI, especially GPAI.[100] NAIS 2.0 clearly recognizes that there are security risks associated with AI, but it places relatively little emphasis on threats to national security. According to NAIS 2.0, the government of Singapore wants to retain agility in its approach to regulating AI, a position backed by public statements by senior government figures. Singapore's approach to AI regulation is sectoral and based, at least for the time being, on existing regulatory frameworks. Singapore's regulatory bodies have been actively incorporating AI into their toolkits, most notably through the Model AI Governance Framework jointly issued by the information communications and data-protection regulators in 2019 and updated in 2020.[101] The framework is aimed at private-sector organizations developing or deploying AI in their businesses. It provides guidance on key ethical and governance issues and is supported by a practical Implementation and Self-Assessment Guide and Compendium of Use Cases to make it easier for companies to map the sector- and technology-agnostic framework onto their organizations.[102] Singaporean regulators have begun to issue sector-specific guidelines for AI, including the advisory guideline on the use of personal data for AI systems that provide recommendations, predictions, and decisions.[103] Like the wider framework, these are non-binding and do not expand the enforcement powers of existing regulators.

Singapore has leaned heavily on technology industry partnerships in developing other elements of its regulatory toolkit, especially its flagship AI Verify product.[104] AI Verify is a voluntary governance testing framework and toolkit that aims to help companies objectively verify their systems against a set of global AI governance and ethical frameworks so that participating firms can demonstrate to users that the companies have implemented AI responsibly. AI Verify works

98 Yeong Zee Kin, "Singapore's Model Framework Balances Innovation and Trust in AI," Organisation for Economic Co-operation and Development, June 24, 2020, https://oecd.ai/en/wonk/singapores-model-framework-to-balance-innovation-and-trust-in-ai.

99 Kayla Goode, Heeu Millie Kim, and Melissa Deng, "Examining Singapore's AI Progress," Center for Security and Emerging Technology, March 2023, https://cset.georgetown.edu/publication/examining-singapores-ai-progress.

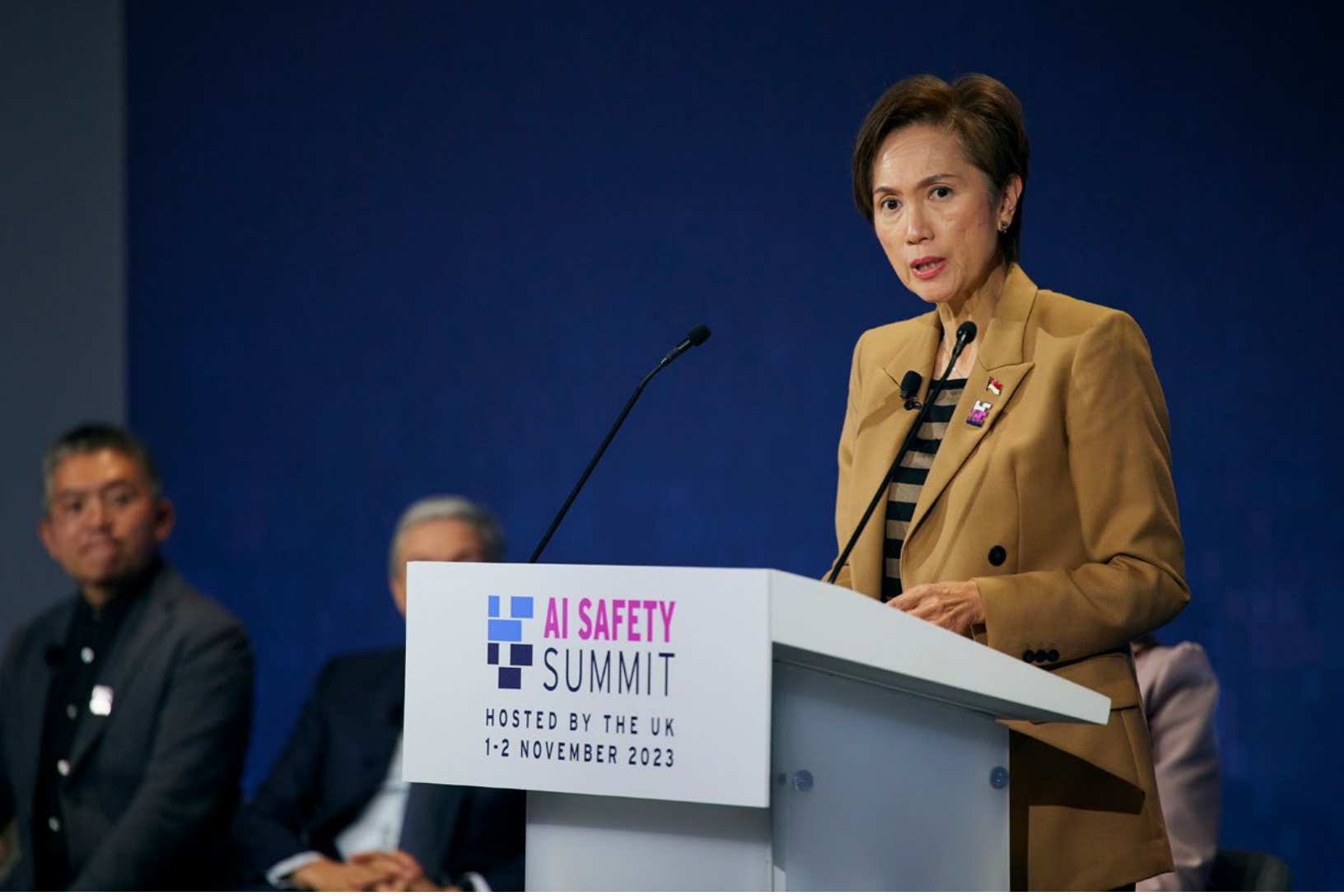
100 "National AI Strategy," Government of Singapore, 2019, https://www.smartnation.gov.sg/nais; Yin Ming Ho, "Singapore's National Strategy in the Global Race for AI," Regional Programme Political Dialogue Asia, February 26, 2024, https://www.kas.de/en/web/politikdialog-asien/digital-asia/detail/-/content/singapore-s-national-strategy-in-the-global-race-for-ai.

101 "Model AI Governance Framework Second Edition," Personal Data Protection Commission of Singapore, January 21, 2020, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf.

102 "Singapore's Approach to AI Governance," Personal Data Protection Commission, last visited January 11, 2025, https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework.

103 "Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems," Personal Data Protection Commission, last visited January 11, 2025, https://www.pdpc.gov.sg/guidelines-and-consultation/2024/02/advisory-guidelines-on-use-of-personal-data-in-ai-recommendation-and-decision-systems.

104 "AI Verify Foundation," AI Verify Foundation, January 9, 2025, https://aiverifyfoundation.sg/ai-verify-foundation.



Josephine Teo, second minister for home affairs of Singapore, spoke at the AI safety summit hosted by the United Kingdom in 2023. Source: Marcel Grabowski/UK Government

within a company's own digital enterprise environment and, as a self-testing and self-reporting toolkit, it has no enforcement power.[105] However, the government of Singapore hopes that, by helping to identify commonalities across various global AI governance frameworks and regulations, it can build a baseline for future international regulations.[106] One critical limitation of AI Verify is that it cannot test GPAI models.[107] The AI Verify Foundation, which oversees AI Verify, recognized this limitation and recently conducted a public consultation to expand the 2020 Model AI Governance Framework to explicitly cover generative AI.[108] The content of the final product is not yet known, and there is no indication that the government intends to translate this new framework into a bespoke AI law, but the consultation document gives important clues about how Singapore is thinking about issues such as accountability; data, including issues of copyright; testing and assurance; and content provenance.[109]

As mentioned, the government of Singapore places relatively little emphasis on national security in its AI policy documents, but that does not mean it is not interested or investing in AI for military and wider national security purposes.[110] In 2022,

105 Marcus Evans, et al., "Singapore Contributes to the Development of Accessible AI Testing and Accountability Methodology with the Launch of the AI Verify Foundation and AI Verify Testing Tool," Data Protection Report, June 15, 2023, https://www.dataprotectionreport.com/2023/06/singapore-contributes-to-the-development-of-accessible-ai-testing-and-accountability-methodology-with-the-launch-of-the-ai-verify-foundation-and-ai-verify-testing-tool.

106 Yeong Zee Kin, "Singapore's A.I.Verify Builds Trust through Transparency," Organisation for Economic Co-operation and Development, August 16, 2022, https://oecd.ai/en/wonk/singapore-ai-verify.

107 "What Is AI Verify?" AI Verify Foundation, last visited January 11, 2025, https://aiverifyfoundation.sg/what-is-ai-verify.

108 "Model AI Governance Framework for Generative AI," AI Verify Foundation, May 30, 2024, https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf.

109 Bryan Tan, "Singapore Proposes Framework for Generative AI," Reed Smith, January 24, 2024, https://www.reedsmith.com/en/perspectives/2024/01/singapore-proposes-framework-for-generative-ai.

110 The phrase "national security" appears only once in the Generative AI proposal and not at all in the NAIS 2.0.

Singapore became the first country to establish a separate military service to address threats in the digital domain.[111] Unlike in the United States, where cyber and other digital specialties are spread across the traditional services, the Digital and Intelligence Service (DIS) brings together the whole domain, from command, control, communications, and cyber operations to implementing strategies for cloud computing and AI.[112] The DIS also has specific authority to raise, train, and sustain digital forces.[113] Within the DIS, the Digital Ops-Tech Centre is responsible for developing AI technologies, but publicly available information about it is sparse.[114] Singapore has deployed AI-enabled technologies through the DIS on exercises, and the Defence Science and Technology Agency (DSTA) has previously stated that it wants to integrate AI into operational platforms, weapons, and back-office functions, but the Singaporean Armed Forces have not published any official position on the use of AI in military systems.[115]

4.5.3 International efforts

Singapore is increasingly taking on a regional leadership role on AI regulation. As chair of the 2024 Association of South-East Asian Nations (ASEAN) Digital Ministers' Meeting, Singapore was instrumental in developing the ASEAN Guide on AI Governance and Ethics.[116] The guide aims to establish common principles and best practices for trustworthy AI in the region but does not attempt to force a common regulatory approach. In part, this is because the ASEAN region is so politically diverse that it would be almost impossible to reach agreement on hot-button issues like censorship, but also because member countries are at wildly different levels of digital maturity.[117] At the headline level, the guide bears significant similarity to US, EU, and UK policies, in that it takes a risk-based approach to governance, but the guide makes concessions to national cultures in a way that those other approaches do not.[118] It is possible that some ASEAN nations might move toward a more stringent EU-style regulatory framework in the future. But, as the most mature AI power in the region, Singapore and its pro-innovation approach will likely remain influential for now.

111 Germany established its Cyber and Information Domain Service in 2016, but it was not upgraded to a separate military service until 2024. "Establishment of the Digital and Intelligence Service: A Significant Milestone for the Next Generation SAF," Government of Singapore, October 28, 2022, https://www.mindef.gov.sg/news-and-events/latest-releases/28oct22_nr2.

112 Mike Yeo, "Singapore Unveils New Cyber-Focused Military Service," C4ISRNet, November 2, 2022, https://www.c4isrnet.com/cyber/2022/11/02/singapore-unveils-new-cyber-focused-military-service.

113 "Fact Sheet: The Digital and Intelligence Service," Singapore Ministry of Defence, October 28, 2022, https://www.mindef.gov.sg/news-and-events/latest-releases/28oct22_fs.

114 "Fact Sheet: Updates to the Establishment of the Digital and Intelligence Service," Singapore Ministry of Defence, June 30, 2022, https://www.mindef.gov.sg/news-and-events/latest-releases/30jun22_fs2.

115 "How Singapore's Defence Tech Uses Artificial Intelligence and Digital Twins," Singapore Defence Science and Technology Agency, November 19, 2021, https://www.dsta.gov.sg/whats-on/spotlight/how-singapore-s-defence-tech-uses-artificial-intelligence-and-digital-twins; Ridzwan Rahmat, "Singapore Validates Enhanced AI-Infused Combat System at US Wargames," *Janes*, September 22, 2023, https://www.janes.com/defence-news/news-detail/singapore-validates-enhanced-ai-infused-combat-system-at-us-wargames.

116 David Hutt, "AI Regulations: What Can the EU Learn from Asia?" Deutsche Welle, August 2, 2024, https://www.dw.com/en/ai-regulations-what-can-the-eu-learn-from-asia/a-68203709.

117 Sheila Chiang, "ASEAN Launches Guide for Governing AI, but Experts Say There Are Challenges," CNBC, February 2, 2024, https://www.cnbc.com/2024/02/02/asean-launches-guide-for-governing-ai-but-experts-say-there-are-challenges.html.

118 Eunice Lim, "Global Steps to Build Trust: ASEAN's New Guide to AI Governance and Ethics," *Workday Blog*, February 9, 2024, https://blog.workday.com/en-hk/2024/global-steps-build-trust-aseans-new-guide-ai-governance-ethics.html.

5: INTERNATIONAL REGULATORY INITIATIVES

At the international level, four key organizations have taken steps into the AI regulation waters—the UN, OECD, the G7 through its Hiroshima Process, and NATO.

5.1 OECD

The OECD published its AI Principles in 2019, and they have since been agreed upon by forty-six countries, including all thirty-eight OECD member states.[119] Though not legally binding, the OECD principles have been extremely influential, and it is possible to trace the five broad topic areas through all of the national and supranational approaches discussed previously.[120] The OECD also provides the secretariat for the Global Partnership on AI, an international initiative promoting responsible AI use through applied co-operation projects, pilots, and experiments.[121] The partnership covers a huge range of activity through its four working groups, and, though defense and national security do not feature explicitly, there are initiatives that could be influential in other forums that consider those areas. For example, the Responsible AI working group is developing technical guidelines for implementation of high-level principles that will likely influence the UN and the G7, and the Data Governance working group is producing guidelines on co-generated data and intellectual-property considerations that could have an impact on the legal use of data for training algorithms.[122] Beyond these specific areas of interest, the OECD will likely remain influential in the wider AI regulation debate, not least because it has built a wide network of technical and policy experts to draw from. This value was seen in practice when the G7 asked the Global Partnership on AI to assist in developing the International Guiding Principles on AI and a voluntary Code of Conduct for AI developers that came out of the Hiroshima Process.[123]

Regulatory approach
The approach is horizontal and risk based.

Scope of regulation
Regulation applies to AI systems and associated knowledge. In theory, this scope covers the whole stack.

There is some specific consideration of algorithms and data through the Global Partnership on AI.

Type of regulation
Regulation is soft, with no compliance regime or enforcement mechanism.

Target of regulation
"AI actors" include anyone or any organization that plays an active role in the AI system life cycle.

Coverage of defense and national security
None.

5.2 G7

The G7 established the Hiroshima AI Process in 2023 to promote guardrails for GPAI systems at a global level. The Comprehensive Policy Framework agreed to by the G7 digital and technology ministers later that year includes a set of International Guiding Principles on Artificial Intelligence and a voluntary Code of Conduct for GPAI developers.[124] As with the OECD AI Principles on which they are largely based, neither of these documents is legally binding. However, by choosing to focus on practical tools to support development of trustworthy AI, the Hiroshima Process will act as a benchmark for countries developing their

119 "The OECD Artificial Intelligence (AI) Principles," Organisation for Economic Co-operation and Development, 2019, https://oecd.ai/en/ai-principles.

120 The five topic areas are: inclusive growth and sustainable development; human-centered values and fairness; transparency and explainability; robustness, security, and safety; and, accountability.

121 "About GPAI," Global Partnership on Artificial Intelligence, 2020, https://gpai.ai/about.

122 "Responsible AI Working Group Report," Organisation for Economic Co-operation and Development, December 2023, https://gpai.ai/projects/responsible-ai/Responsible%20AI%20WG%20Report%202023.pdf; "Data Governance Working Group Report," Global Partnership on Artificial Intelligence, December 2023, https://gpai.ai/projects/data-governance/Data%20Governance%20WG%20Report%202023.pdf.

123 "OECD Launches Pilot to Monitor Application of G7 Code of Conduct on Advanced AI Development," Organisation for Economic Co-operation and Development, July 22, 2024, https://www.oecd.org/en/about/news/press-releases/2024/07/oecd-launches-pilot-to-monitor-application-of-g7-code-of-conduct-on-advanced-ai-development.html.

124 "G7 Leaders' Statement on the Hiroshima AI Process," European Commission, October 30, 2023, https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process.

own regulatory frameworks.[125] There is some evidence that this is already happening and a suggestion that the EU might adopt a matured version of the Hiroshima Code of Conduct as part of its AI Act compliance regime.[126] That will require input from the technology sector, including current and future suppliers of AI for defense and national security.

The G7 is also taking a role in other areas that might impact AI regulation, most notably technical standards and international data flows. On the former, the G7 could theoretically play a coordination role in ensuring that disparate national standards do not lead to an incoherent regulatory landscape that is time consuming and expensive for the industry to navigate.[127] However, diverging positions even within the G7 might make that difficult.[128] The picture emerging in the international data flow space is only a little more optimistic. The G7 has established a new Institutional Arrangement for Partnership (IAP) to support its Data Free Flow with Trust (DFFT) initiative, but it has not yet produced any tangible outcomes.[129] The EU-US Data Privacy Framework has made some progress in reducing the compliance burden associated with cross-border transfer of data through the EU-US Data Bridge and its UK-US extension, but there is still a large risk that the Court of Justice of the European Union will strike it down over concerns that it violates GDPR.[130]

Regulatory approach

The approach is vertical. The Hiroshima Code of Conduct applies only to general-purpose AI.

Scope of regulation

The scope is GPAI systems, with significant focus on data, particularly data sharing and cross-border transfer.

Type of regulation

Regulation is soft, with no compliance regime or enforcement mechanism.

Target of regulation

Developers of GPAI are the only target.

Coverage of defense and national security

None.

125 Hiroki Habuka, "The Path to Trustworthy AI: G7 Outcomes and Implications for Global AI Governance," Center for Strategic and International Studies, June 6, 2023, https://www.csis.org/analysis/path-trustworthy-ai-g7-outcomes-and-implications-global-ai-governance.

126 Gregory C. Allen and Georgia Adamson, "Advancing the Hiroshima AI Process Code of Conduct under the 2024 Italian G7 Presidency: Timeline and Recommendations," Center for Strategic and International Studies, March 27, 2024, https://www.csis.org/analysis/advancing-hiroshima-ai-process-code-conduct-under-2024-italian-g7-presidency-timeline-and.

127 Habuka, "The Path to Trustworthy AI: G7 Outcomes and Implications for Global AI Governance."

128 Peter J. Schildkraut, "The Illusion of International Consensus—What the G7 Code of Conduct Means for Global AI Compliance Programs," Arnold & Porter, January 18, 2024, https://www.arnoldporter.com/en/perspectives/publications/2024/01/what-the-g7-code-of-conduct-means-for-global-ai-compliance.

129 "Ministerial Declaration—G7 Industry, Technology, and Digital Ministerial Meeting," Group of Seven, 2024, https://www.g7italy.it/en/eventi/industry-tech-and-digital/.

130 Joe Jones, "UK-US Data Bridge Becomes Law, Takes Effect 12 Oct.," International Association of Privacy Professionals, August 21, 2023, https://iapp.org/news/a/uk-u-s-data-bridge-becomes-law-takes-effect-12-october; Camille Ford, "The EU-US Data Privacy Framework Is a Sitting Duck. PETs Might Be the Solution," Centre for European Policy Studies, February 23, 2024, https://www.ceps.eu/the-eu-us-data-privacy-framework-is-a-sitting-duck-pets-might-be-the-solution.

5.3 United Nations

The UN has been cautious in its approach to AI regulation. The UN Educational, Scientific, and Cultural Organization (UNESCO) issued its global standard of AI ethics in 2021 and established the AI Ethics and Governance Lab to produce tools to help member states asses their relative preparedness to implement AI ethically and responsibly, but these largely drew on existing frameworks rather than adding anything new.[131] Interest in the area ballooned following the release of ChatGPT, such that Secretary-General António Guterres convened an AI Advisory Body in late 2023 to provide guidance on future steps for global AI governance. That report, published in late 2024 and titled "Governing AI for Humanity," did not recommend a single governance model, but it proposed establishing a regular AI policy dialogue within the UN to be supported by an international scientific panel of AI experts.[132] Specific areas of concern include the need for consistent global standards for AI and data, and mechanisms to facilitate inclusion of the Global South and other currently underrepresented groups in the international dialogue on AI.[133] A small AI office will be established within the UN Secretariat to coordinate these efforts.

At the political level, the General Assembly has adopted two resolutions on AI. The first, Resolution 78/L49 on the promotion of "safe, secure and trustworthy" artificial AI systems, was drafted by the United States but drew co-sponsorship support from a wide range of countries, including some in the Global South.[134] The second, Resolution 78/L86, drafted by China and supported by the United States, calls on developed countries to help developing countries strengthen their AI capacity building and enhance their representation and voice in global AI governance.[135] Adoption of both resolutions by consensus could indicate global support for Chinese and US leadership on AI regulation, but the depth of that support remains unclear.[136] Notably, following the adoption of Resolution 78/L86, two separate groups were established, one led by the United States and Morocco, and the other by China and Zambia.[137]

There is also disagreement over the role of the UN Security Council (UNSC) in addressing AI-related threats. Resolution 78/L49 does not apply to the military domain but, when introducing the draft, the US permanent representative to the UN suggested that it might serve as a model for dialogue in that area, albeit not at the UNSC.[138] The UNSC held its first formal meeting focused on AI in July 2023.[139] In his remarks, the secretary-general noted that both military and non-military applications of AI could have implications for global security and welcomed the idea of a new UN body to govern AI, based on the model of the International Atomic Energy Agency.[140] The council has since expressed its commitment to consider the international security implications of scientific advances more systematically, but some members have raised concerns about framing the issue narrowly within a security context. At the time of writing, this remains a live issue.[141]

131 "Ethics of Artificial Intelligence," UNESCO, 2024, https://www.unesco.org/en/artificial-intelligence/recommendation-ethics; "Global AI Ethics and Governance Observatory," UNESCO, 2021, https://www.unesco.org/ethics-ai/en.

132 "Governing AI for Humanity," United Nations, September 19, 2024, https://www.un.org/Sites/Un2.Un.org/Files/Governing_ai_for_humanity_final_report_en.pdf.

133 Tess Buckley, "Governing AI for Humanity: UN Report Proposes Global Framework for AI Oversight," TechUK, September 20, 2024, https://www.techuk.org/resource/governing-ai-for-humanity-un-report-proposes-global-framework-for-ai-oversight.html; Alexander Amato-Cravero, "UN Releases Its Final Report on 'Governing AI for Humanity,'" Herbert Smith Freehills, October 8, 2024, https://www.herbertsmithfreehills.com/notes/tmt/2024-posts/UN-releases-its-final-report-on--Governing-AI-for-Humanity-.

134 "General Assembly Adopts Landmark Resolution on Artificial Intelligence," United Nations, March 21, 2024, https://news.un.org/en/story/2024/03/1147831.

135 "Enhancing International Cooperation on Capacity-Building of Artificial Intelligence," United Nations, June 25, 2024, https://documents.un.org/doc/undoc/ltd/n24/183/80/pdf/n2418380.pdf.

136 Edith Lederer, "UN Adopts Chinese Resolution with US Support on Closing the Gap in Access to Artificial Intelligence," Associated Press, July 2, 2024, https://apnews.com/article/un-china-us-artificial-intelligence-access-resolution-56c559be7011693390233a7bafb562d1.

137 "Artificial Intelligence: High-Level Briefing," Security Council Report, December 18, 2024, https://www.securitycouncilreport.org/whatsinblue/2024/12/artificial-intelligence-high-level-briefing.php.

138 Linda Thomas-Greenfield, "Remarks by Ambassador Thomas-Greenfield at the UN Security Council Stakeout Following the Adoption of a UNGA Resolution on Artificial Intelligence," United States Mission to the United Nations, March 21, 2024, https://usun.usmission.gov/remarks-by-ambassador-thomas-greenfield-at-the-un-security-council-stakeout-following-the-adoption-of-a-unga-resolution-on-artificial-intelligence.

139 "July 2023 Monthly Forecast: Security Council Report," Security Council Report, July 2, 2023, https://www.securitycouncilreport.org/monthly-forecast/2023-07/artificial-intelligence.php.

140 Michelle Nichols, "UN Security Council Meets for First Time on AI Risks," Reuters, July 18, 2023, https://www.reuters.com/technology/un-security-council-meets-first-time-ai-risks-2023-07-18.

141 "Statement by the President of the Security Council," United Nations, September 21, 2024, https://documents.un.org/doc/undoc/gen/n24/307/20/pdf/n2430720.pdf; "July 2023 Monthly Forecast: Security Council Report."

Source: NATO

Regulatory approach
The approach is horizontal with a focus on the Sustainable Development Goals.

Scope of regulation
AI systems are broadly defined, with particular focus on data governance and avoiding biased data.

Type of regulation
Regulation is soft, with no compliance regime or enforcement mechanism.

Target of regulation
Resolutions refer to design, development, deployment, and use of AI systems.

Coverage of defense and national security
Resolutions exclude military use, but there have been some discussions in the UNSC.

5.4 NATO

NATO is not in the business of civil regulation, but it plays a major role in military standards and is included here for completeness.

The Alliance formally adopted its first AI strategy in 2021, well before the advent of ChatGPT and other forms of GPAI.[142] At that time, it was not clear how NATO intended to overcome different approaches to governance and regulatory issues among allies, nor was it obvious which of the many varied

142 "Summary of the NATO Artificial Intelligence Strategy," NATO, October 22, 2021, https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

NATO bodies with an interest in AI would take the lead.[143] The regulatory issue has, in some ways, become more settled with the advent of the EU's AI Act, in that the gaps between European and non-European allies are clearer. Within NATO itself, the establishment of the Data and Artificial Intelligence Review Board (DARB) under the auspices of the assistant secretary-general for innovation, hybrid, and cyber places leadership of the AI agenda firmly within NATO Headquarters rather than NATO Allied Command Transformation.[144] One of the DARB's first priorities is to develop a responsible AI certification standard to ensure that new AI projects meet the principles of responsible use set out in the 2021 AI Strategy.[145] Though this certification standard has not yet been made public, NATO is clearly making some progress in building consensus across allies. However, NATO is not a regulatory body and has no enforcement role, so it will require member states to self-police or transfer that enforcement role to a third-party organization.[146]

NATO requires consensus to make decisions and, with thirty-two members, consensus building is not straightforward or quick, especially on contentious issues. Technical standards might be easier for members to agree on than complex, normative issues, and technical standards are an area in which NATO happens to have a lot of experience.[147] The NATO Standardization Office (NSO) is often overlooked in discussions of the Alliance's successes, but its work to develop, agree to, and implement standards across all aspects of the Alliance's operational and capability development has been critical.[148] As the largest military standardization body in the world, NSO is uniquely placed to determine which civilian AI standards apply to military and national security use cases and identify areas where niche standards are needed.

Regulatory approach
The approach is horizontal. AI principles apply to all types of AI.

Scope of regulation
AI systems are broadly defined.

Type of regulation
Regulation is soft. NATO has no enforcement mechanism, but interoperability is a key consideration for member states and might drive compliance.

Target of regulation
The target is NATO member states developing and deploying AI within their militaries.

Coverage of defense and national security
The regulation is exclusively about this arena.

143 Simona Soare, "Algorithmic Power, NATO and Artificial Intelligence," *Military Balance Blog*, November 19, 2021, https://www.iiss.org/ja-JP/online-analysis/military-balance/2021/11/algorithmic-power-nato-and-artificial-intelligence.

144 "NATO Allies Take Further Steps Towards Responsible Use of AI, Data, Autonomy and Digital Transformation," NATO, October 13, 2022, https://www.nato.int/cps/en/natohq/news_208342.htm.

145 "NATO Starts Work on Artificial Intelligence Certification Standard," NATO, February 7, 2023, https://www.nato.int/cps/en/natohq/news_211498.htm.

146 Daniel Fata, "NATO's Evolving Role in Developing AI Policy," Center for Strategic and International Studies, November 8, 2022, https://www.csis.org/analysis/natos-evolving-role-developing-ai-policy.

147 Maggie Gray and Amy Ertan, "Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment," NATO Cooperative Cyber Defence Centre of Excellence, NATO, January 2021, https://ccdcoe.org/library/publications/artificial-intelligence-and-autonomy-in-the-military-an-overview-of-nato-member-states-strategies-and-deployment.

148 "Standardization," NATO, October 14, 2022, https://www.nato.int/cps/en/natohq/topics_69269.htm.

6: ANALYSIS

The regulatory landscape described above is complex and constantly evolving, with big differences in approach seen even between otherwise well-aligned countries. However, by breaking various approaches into their component parts, it is possible to see some common themes.

6.1 Common themes

6.1.1 Regulatory approach

The general preference seems to be for a sectoral or use-case-based approach, framed as a pragmatic attempt to balance competing requirements to promote innovation while protecting users. However, there is increasing concern that some kinds of AI, notably large language models and other forms of GPAI, should be regulated with a vertical, technology-based approach. China looks like an outlier here, in that its approach is vertical with horizontal elements rather than the other way around, but in practice the same regulatory ground could be covered.

6.1.2 Scope

There is little consensus around which elements of AI should be regulated. In cases where the framework refers simply to "AI systems" without saying explicitly whether that includes training data, specific algorithms, packaged applications, etc., it is possible to infer the intended scope through references in implementation guidance and other documentation. This approach makes sense in jurisdictions where the regulatory approach relies on existing sectoral regulators with varying focus. For example, a regulator concerned with the delivery of public utilities might be concerned with the applications deployed by the utilities providers, whereas a financial services regulator might need to look deeper into the stack to consider the underlying data and algorithms. China is again the outlier, as its regulation is specifically focused on the algorithmic level, with some coverage of training data in specific cases.

6.1.3 Type of regulation

The EU and China are, so far, the only jurisdictions to have put in place hard regulations specifically addressing AI. Most other frameworks rely on existing sectoral regulators incorporating AI into their work, voluntary guidelines and best practices, or a combination of both. It is possible that the EU's AI Act will become a model as countries increasingly turn to a legislative approach, but practical concerns and lengthy timelines mean that most compliance and enforcement regimes will remain fragmented for now.

6.1.4 Target group

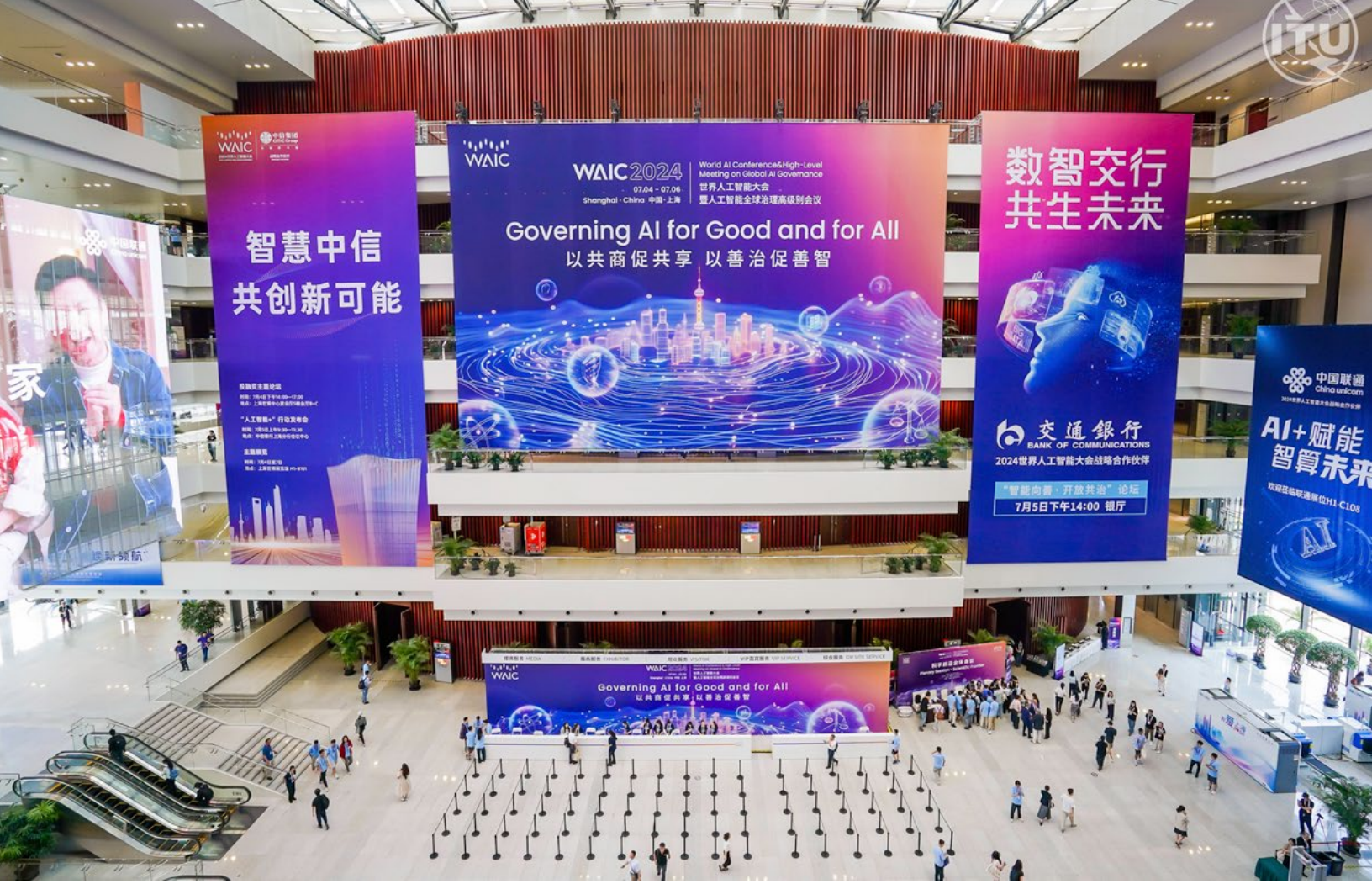
Almost all of the frameworks place some degree of responsibility on developers of AI systems, albeit voluntarily in the loosest arrangements. Deployers of AI systems and the service providers that make them available are less widely included. There is some suggestion that assignment of responsibility might vary across the AI life cycle, though what this means in practice is unclear, and only Singapore suggests differentiating between ex ante and ex post responsibility. Even in cases in which responsibility is clearly ascribed, it is likely that questions of legal liability for misuse or harm will take time to be worked out through the relevant judicial system. China is again an outlier here, but a more comprehensive AI law could include developers and deployers.

6.2 Impact on defense and national security

At first glance, little of the civil regulatory frameworks discussed above relates directly to the defense and national security community, but there are at least three broad areas in which the defense and national security community might be subject to second-order or unintended consequences.

- Market-shaping civil regulations could affect the tools available to the defense and national security community. This area could include direct market interventions, such as modifications to antitrust law that might force incumbent suppliers to break up their companies, or second-order implications of interventions that affect the sorts of skills available in the market, the sorts of problems that skilled AI workers want to work on, and the data available to them.

- Judicial interpretation of civil regulations could impact the defense and national security communities' license to operate, either by placing direct limitations on the use of AI in specific use cases, such as domestic counterterrorism, or more indirectly through concerns around legal liability.



China hosted the World AI Conference & High-Level Meeting on Global AI Governance in Shanghai in 2024. Source: ITU

- Regulations could add hidden cost or risk to the development and deployment of AI systems for defense and national security use. This area could include complex compliance regimes or fragmented technical standards that must be paid for somewhere in the value chain, or increased security risks associated with licensing or reporting of dual-use models.

By using these areas as lenses through which to assess the tools and approaches found within civil regulatory frameworks, it is possible to begin picking out specific areas and initiatives of concern to the defense and national security community. The tables below make an initial assessment of the potential implications of civil regulation of AI on the defense and national security community by grouping them into three buckets.

- **Be supportive:** Areas or initiatives that the community should get behind and support in the short term.
- **Be proactive:** Areas that are still maturing but in which greater input is needed and the impact on the community could be significant in the medium term.
- **Be watchful:** Areas that are still maturing but in which uncertain future impacts could require the community's input.

The content of these tables is by no means comprehensive, but it gives an indication of areas in which the defense and national security community might wish to focus its resources and attention while the civil regulatory landscape continues to develop.

BE SUPPORTIVE **Areas or initiatives that the community should get behind and support in the short term**	
Technical standards	Defense and national security technical standards should, as far as possible, align with civil-sector standards to minimize the cost of compliance, maximize interoperability, and allow efficient adoption of civil solutions to specialist problems. ACTION ON: **chief information officers, chief AI officers, standard-setting bodies, and AI developers in the public and private sectors.**
Risk-assessment tools	Adopting tools and best practices developed in the civil sector could save time and money that could be better spent on advancing capability or readiness. ACTION ON: **chief information officers, chief AI officers, and risk-management professionals including auditors, system integrators, and AI developers in the public and private sectors.**
Safety and assurance tools	As above, adopting tools and best practices developed in the civil sector could be more efficient, but there could also be reputational and operational benefits to equivalency in some areas like aviation, in which military and civil users of AI systems might need to share airspace. ACTION ON: **chief information officers, chief AI officers, compliance officers, and domain safety specialists.**

BE PROACTIVE **Areas that are still maturing but in which greater input is needed and the impact on the community could be significant in the medium term**	
Regulation of adjacent sectors and use cases	Restrictions on the use of AI in domestic security and policing could limit development of capabilities of use to the defense and national security community or increase the cost of capabilities by limiting economies of scale. This is especially concerning in technically complex areas such as counterterrorism, covert surveillance and monitoring, and pattern detection for intelligence purposes. ACTION ON: **chief information officers, chief AI officers, legal and operational policy advisers, and AI developers in the public and private sectors.**
Data sharing and transfer	Regulatory approaches that impact, in policy or practical terms, the ability of the defense and national security community to share data between allies across national borders could limit or impose additional costs on collaborative capability development and deployment. ACTION ON: **chief information officers, chief AI officers, data-management specialists, and export-control policymakers.**
Special regulatory provisions for generative AI	Regulations placed on the general-purpose AI systems that underpin sector-specific applications could impact the capabilities available to defense and national security users, even if those use cases are themselves technically exempt from such restrictions. ACTION ON: **chief information officers, chief AI officers, standard-setting bodies, legal and operational policy advisers, and AI developers in the public and private sectors.**

BE WATCHFUL

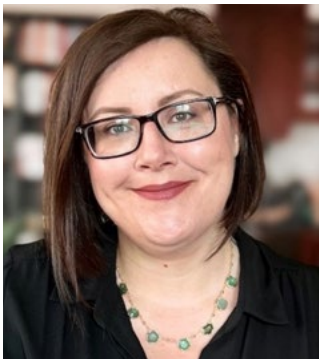
Areas that are still maturing but in which uncertain future impacts could require the community's input

Licensing and registration databases	Such databases could easily exclude algorithms and models developed specifically for defense or national security purposes. However, registering the open-source or proprietary models on which those tools are based could still pose a security risk if malign actors accessed the registry. ACTION ON: **chief information officers, chief AI officers, risk-management professionals, and counterintelligence and security policymakers.**
Data protection, privacy, and copyright regulations	AI systems do not work without data. Domestic regulation of privacy, security, and rights-impacting data, as well as interpretations of fair use in existing copyright law, could limit access to training data for future AI systems. ACTION ON: **chief information officers, chief AI officers, privacy and data-protection professionals, and AI developers in the public and private sectors.**
Market-shaping regulation	The AI industry, especially at the cutting edge of general-purpose AI, is heavily dominated by a few incumbents, most of which operate internationally. Changes to the substance or interpretation of domestic antitrust regulations could impact the supply base available to the defense and national security community. ACTION ON: **chief information officers, chief AI officers, commercial policymakers, and legal advisers.**
Legal liability	Like any other capability, AI systems used by the military and national security community in an operational context are covered by the law of armed conflict and broader international humanitarian law, not domestic legislation. However, in nonoperational contexts, judicial interpretation of civil laws could impact particularly questions of criminal, contractual, or other liability. ACTION ON: **chief information officers, chief AI officers, and legal and operational policy advisers.**

7: CONCLUSION

The AI regulatory landscape is complex and fast-changing, and likely to remain so for some time. While most of the civil regulatory approaches described here exclude defense and national security applications of AI, the intrinsic dual-use nature of AI systems means that the defense and national security community cannot afford to think of or view itself in isolation. This paper has attempted to look beyond the rules and regulations that the community chooses to place on itself to identify areas in which the boundary with civil-sector regulation is most porous. In doing so, this paper has demonstrated that regulatory carve-outs for defense and national security uses must be part of a broader solution ensuring the community's needs and perspectives are incorporated into civil frameworks. The areas of concern identified are just a first cut of the potential second-order and unintended consequences that could limit the ability of the United States and its allies to reap the rewards that AI offers as an enhancement to military capability on and off the battlefield. Private-sector AI firms with dual-use products, industry groups, government offices with national security responsibility for AI, and legislative staff should use this paper as a roadmap to understand the impact of civil AI regulation on their equities and plan to inject their perspectives into the debate.

AUTHOR BIOGRAPHY



Deborah Cheverton is a nonresident senior fellow in the Atlantic Council's *Forward* Defense program within the Scowcroft Center for Strategy and Security. Cheverton is a senior trade and investment adviser with the UK embassy, where she works on foreign direct investment in support of bilateral and multilateral defense and security priorities. Before working in trade, she worked for the United Kingdom's Ministry of Defence (MOD) for fifteen years, working across a range of policy and delivery areas with a particular focus on science and technology policy, industrial strategy, capability development, and international collaboration.

Cheverton's research interests center around the impact of advancements in digital and other emerging technologies on conflict and competition, as well as the industrial and international collaboration issues that follow. Prior to her Atlantic Council fellowship, she served as private secretary to the second permanent secretary of the MOD, playing a key role in driving innovation and pace into the digital, data, and modernization agenda. Previous roles include leading the communications and engagement team working on the 2021 UK Integrated Review, two years as a private secretary to the UK minister for defence procurement, and three years in the British Defence Staff in Washington, DC, where she was an early advocate for the United Kingdom's approach to innovation in its 2015 Strategic Defence and Spending Review. Cheverton began her career as an analyst in the UK's Defence Science and Technology Laboratory and was deployed to Afghanistan in that capacity in 2013.

She holds a master's degree in physics from the University of Manchester and a bachelor's with honors in international relations from the Open University.

ACKNOWLEDGEMENTS

This paper would not have been possible without help and constructive challenge from the entire staff of the *Forward* Defense program, especially the steadfast support of Clementine Starling-Daniels, the editorial and grammatical expertise of Mark Massa, and the incredible patience of Abigail Rudolph.

Atlantic Council

Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street, NW, 11th Floor
Washington, DC 20005

www.AtlanticCouncil.org