

Policy Brief No. 218 – December 2025

Trust by Design? AI in Military Applications

Branka Marijan

Key Points

- Military adoption of artificial intelligence (AI) is outpacing governance, compressing decision time and heightening escalation risk. In response, “trust” must be operationalized as assured reliance, clear claims, evidence and accountability — at system, organizational and interstate levels.
- “Trust-by-design” frameworks offer possible ways in which to ensure both technical and governance considerations are embedded into the life cycle of AI systems.
- Confidence building measures (CBMs) between states, notably the United States and China, on emerging military technologies are necessary to ensure trust building. CBMs such as mutual declarations of principles, incident notification protocols and joint verification mechanisms are urgently needed to prevent miscalculation and escalation.

Introduction

As rivalries sharpen from Washington to Beijing, a new fault line is emerging: trust in AI. Nowhere is the question more pressing than in military applications and international security discussions. Militaries want systems that soldiers will use, and commanders can rely on. Diplomats want frameworks that can prevent accidents and reassure adversaries. At stake is whether frameworks, such as “trust by design,” can bridge these needs across technology and governance.

The issue of trust in AI extends beyond defence. A 2025 University of Melbourne and KPMG survey of 48,000 people in 47 countries found that more than half, some 54 percent, remain wary of trusting AI (Gillespie et al. 2025). Concerns range from accuracy and bias to contextual blind spots and the risks of misuse. Interestingly, some 70 percent of those respondents see regulation as crucial in addressing the mistrust (ibid.). A calibrated level of trust is essential: too much trust can lead to overreliance on AI, which itself carries risk, including in unexpected ways, such

About the Author

Branka Marijan is a CIGI senior fellow and a senior researcher at Project Ploughshares. She is a lecturer in the Master of Global Affairs program at the Munk School of Global Affairs and Public Policy at the University of Toronto.

At Ploughshares, Branka leads research on the military and security implications of emerging technologies. Her work examines concerns regarding the development of autonomous weapons systems and the impact of artificial intelligence and robotics on security provision. Her research interests include trends in warfare, civilian protection, use of drones and civil-military relations.

She holds a Ph.D. from the Balsillie School of International Affairs with a specialization in conflict and security. She has conducted research on post-conflict societies and published academic articles and reports on the impacts of conflict on civilians and diverse issues of security governance, including security sector reform.

Branka closely follows United Nations disarmament efforts and attends international and national consultations and conferences. She is a board member of the Peace and Conflict Studies Association of Canada and a research fellow at the Kindred Credit Union Centre for Peace Advancement at the University of Waterloo.

as negatively impacting human cooperation (Klingbeil, Grützner and Schreck 2024), while underuse could mean forgoing benefits. Governance has to strike the right balance.

Trust building among states is essential to prevent misperception and miscalculation over AI capabilities and intent. As AI now permeates defence, from policy to on-the-ground execution, confidence-building measures are critical (Puscas 2022; Horowitz and Kahn 2021). Despite several initiatives on responsible military AI applications and autonomous weapons, governance is still lagging the technological developments.

A “trust-by-design” approach aims to address these challenges by embedding frameworks and principles that ensure trustworthiness and ethical standards are integrated across the entire AI life cycle, from development to deployment and use (Merchán-Cruz et al. 2025). In many ways, the trust-by-design framework for AI proposed by scholars such as Emmanuel Merchán-Cruz et al. (2025) among others, for industry, is also relevant in international security discussions. The proposed industry framework encompasses the core principles that have emerged in discussions of responsible military AI and autonomous weapons, notably “human-centricity, transparency, and accountability” (ibid.). This brief then suggests that trust by design is about the system, organization and governance so that reliance is justified, and demonstrably so, via testable properties, enforceable processes and accountable actors. The challenge is that building such a comprehensive framework for international security requires both political will and creativity; there is no ready-made model that states can simply adopt.

Figuring out a way to build out this architecture of trust is precisely what is needed to ensure responsible use of AI in defence, as well as ensure global stability. On a trip to China, Thomas Friedman (2025) observed that trust and governance was particularly necessary between two of the Great Powers, the United States and China. Friedman (2025) goes as far as to say, “Because what Soviet-American nuclear arms control was to world stability since the 1970s, U.S.-Chinese A.I. collaboration to make sure we

effectively control these rapidly advancing A.I. systems will be for the stability of tomorrow's world." Bold though it may sound, the sentiment was echoed soon after by China's disarmament ambassador, Shen Jian, who underscored the need for trust building and multilateralism even as he criticized US export restrictions.

Speaking on a panel at the close of the inaugural Global Conference on AI, Security and Ethics (AISE) hosted by the United Nations Institute for Disarmament Research (UNIDIR) in March 2025, Jian pointed to Friedman's article and issues of trust and trust building between the United States and China. Jian expressed frustration that the United States was constraining China from accessing technologies, such as advanced semiconductors, by pressuring allies not to export to China. Jian suggested a need for states to work together on AI governance while developing a clear "line of national security in terms of export control of high-tech technologies" (Chaulagain 2025). The co-panellists — disarmament ambassadors from Italy, the Netherlands, Pakistan and the Republic of Korea — agreed with Jian on the need for trust building and argued for multilateralism as a response to the distrust. Distrust of AI applications in international security extends well beyond the United States and China, though the two powers remain at the forefront of AI development and competition.

Against this background, this brief examines why trust is even more of a foundational element of global security in the AI era, and how embedding trustworthiness into both technologies and institutions can reduce the risks of miscalculation and escalation. It draws on insights from the AISE conference and other multilateral discussions, where leaders and experts underscore an "Oppenheimer moment" for AI and call for urgent oversight to prevent misuse on the battlefield (Robins-Early 2024). The brief concludes with actionable recommendations: instituting voluntary transparency and reporting mechanisms on military AI, adopting human agency impact assessments to preserve human control, pursuing regional risk-reduction strategies and launching capacity-sharing initiatives. In essence, achieving trust by design in military AI is both a technical and diplomatic endeavour that fixes responsibility on humans and organizations.

Trust as a Cornerstone of Multilateral AI Governance

Trust underpins cooperation in international politics. For military AI, trust has two dimensions: interstate trust — the expectation that other states will use AI in a responsible and predictable way and will uphold commitments; and system trust — confidence that AI tools are reliable, understandable and aligned with legal and ethical constraints.

Heightened geopolitical competition has eroded both. Major powers fear that rivals' advances could confer decisive advantage or be used coercively. Building trust in this context will require incremental confidence building, much as US-Soviet arms control began with small steps. It also demands commitment to transparency and dialogue, with transparency understood as both greater information sharing and clarity on the ways in which systems being developed align with existing laws and new norms (Marijan 2025). International relations scholars define trust as the expectation that another party's intentions are good and that it will act reliably. Where trust is thin, states hesitate to accept constraints and presume worst-case intentions. Technical fixes alone cannot resolve this. Governance measures that create predictability and accountability are essential complements.

These questions are not entirely new in the discussions on military AI and autonomous weapons. Trust and trustworthiness in the application of AI has been a topic of interest to diplomats, technical experts, scholars and analysts for many years (Roff and Danks 2018). Indeed, the United Nations Group of Governmental Experts on Lethal Autonomous Weapons Systems discussions have considered the issue for more than a decade. Still, the topic has gained new urgency given the developments in AI, notably generative AI, where the applications of technology have expanded well beyond weapons to the whole of the military domain.

Consider the use of AI in decision-support systems, which have been used to assist targeting in Gaza and Ukraine. In his address to the AISE conference, UN Secretary-General António

Guterres alluded to these recent conflicts, saying that uses of AI-enabled systems had violated international humanitarian law and harmed civilians, underscoring a new UN General Assembly resolution (79/239) as an important first step toward getting states to assess the risks and opportunities of military AI (Chaulagain 2025). Though Guterres did not state it, one of the key challenges on the uses of AI in decision-support systems has been the lack of transparency and information from states deploying these systems. Rather, much of what is publicly known about the systems is based on journalistic accounts that have raised significant questions regarding the speed in decision making and the actual accuracy of systems used (Abraham 2024). The lack of transparency on AI decision-support systems, both in terms of the actual systems used as well as the process and context in which they are used, has been noted by diplomats and experts as one area states should aim to exchange information on (Marijan 2025).

To foster that expectation with AI, states need more openness about their military AI policies and a willingness to discuss what uses of AI they consider off-limits or risky. Given that AI is an enabler rather a weapon system per se, the ways in which states craft policies and exchange information that leads to norm building and agreements regarding responsible use will be essential (Scharre and Lamberth 2022). As AI evolves, driven largely by industry, international dialogue must be flexible and keep pace with change. Because AI reshapes risk across other weapon and technology domains, including nuclear, chemical and biological, governance should be cross-sector and avoid the silos that often hobble arms-control debates. Finally, amid considerable hype, policy must rest on sober assessments of technical feasibility, operational performance and failure modes (Lindelauf and Meerveld 2025).

International discussions, including the Responsible Artificial Intelligence in the Military Domain (REAIM) summits, provide venues for this broader dialogue. The next REAIM Summit is scheduled for February 2026 in Spain, following earlier gatherings in the Netherlands (2023) and the Republic of Korea (2024). The AISE conference “Trust-Building” panel itself brought together officials from China, France, Italy, the Netherlands, Pakistan and the Republic of Korea. They explored how trust building might proceed despite differing perspectives, identifying areas of shared interest

such as avoiding accidental conflict. Middle-power diplomats (for example, from the Netherlands and the Republic of Korea) often serve as intermediaries, helping to reframe debates in ways that can be acceptable to both Western and non-Western viewpoints. Such inclusive fora are critical. They enable states to voice concerns and clarify intentions, which is the raw material of trust. Over time, repeated interactions — through UN working groups, track 1.5 dialogues and coalition initiatives such as REAIM — can shift perceptions and build shared understanding, reducing the tendency to act on assumptions or misperceptions about others’ use of AI. In short, trust must be cultivated deliberately in the AI arena. It is both an input and an output of successful governance: a prerequisite for states to agree on rules, and the desired result of adhering to those rules. Friedman’s appeal for US-China collaboration on AI captures this duality: without trust, cooperation falters; without cooperation, the technological Wild West deepens mistrust. To break this vicious cycle, states will need to invest political capital in confidence building even as they compete technologically. The next sections discuss how lack of transparency exacerbates risks, and how confidence-building measures can help reverse that dynamic.

The Perils of Distrust: Miscalculation and Escalation Risks

Perhaps the greatest near-term danger posed by the integration of AI into the military domain is unintended escalation — conflict sparked by misunderstanding or miscalculation (Horowitz and Kahn 2021). History is rife with close calls (in nuclear and conventional domains), where misperception nearly led to war. AI could heighten those risks if nations cannot discern what an autonomous system is doing or why or when AI in some way obscures the intentions of operators. The opacity of AI systems — especially complex machine-learning algorithms that even their creators may struggle to explain, the so-called black box problem — means that not only humans *using* AI, but adversaries observing AI-driven actions, might misinterpret behaviour. There is also the issue of brittleness and data drift, where

systems trained for particular contexts and on certain data act unpredictably or fail (Lindelauf and Meerveld 2025). A brittle AI system that falters in unexpected ways on the battlefield could trigger a disproportionate response from an opponent who assumes a deliberate attack. For example, if an autonomous drone strays out of its prescribed zone due to a classification error, the adversary, seeing an incursion, could assume a prelude to wider attack. In a crisis in a sensitive political region, such incidents can escalate with frightening speed.

Moreover, AI accelerates operational tempo and compresses decision windows, increasing pressure on human operators. Reporting on the use of AI decision-support systems in Gaza suggests some operators spent roughly 20 seconds per target, often only to confirm that the target was male (Abraham 2024). Because Israel has not disclosed details of its systems or procedures, it is unclear how representative these accounts are of actual use. If accurate, the operators seemed to have placed a great deal of trust in the targeting recommendations made by AI systems. The episode underscores the need to calibrate trust and for states to share more information about time pressure, operator training and practices, and safeguards. Transparency on decision speeds, escalation controls and limits on autonomy would help reduce risks that AI enables rapid, and potentially excessive, scaling of force. Again, these issues could be addressed by design to ensure that soldiers deploying systems are appropriately trained, that systems are continuously monitored and use is logged and reviewed after incidents.

CBMs: Tools to Foster Trust and Restraint

Throughout the Cold War, adversaries learned that they could reduce the risk of war through CBMs — arrangements to share information, increase transparency and clarify intentions. Today, CBMs are gaining recognition as a flexible tool set to address AI-related security dilemmas (Puscas 2022; Horowitz and Kahn 2021). In essence, CBMs are trust building by design: they deliberately inject predictability into a volatile environment. During the Cold War, measures such as data exchanges, notification of military exercises and observation visits were

employed to assure each side that routine activities were not cover for an attack. Applied to AI, CBMs might include sharing national policy white papers on military AI use; notifying others about major tests or deployments of certain autonomous systems; exchanging observers for international AI exercises or competitions; or jointly developing a glossary of AI terms to prevent misunderstandings.

Indeed, voluntary reporting mechanisms could be an outgrowth of this process, where states periodically share updates on steps taken to ensure their military AI is safe, explainable and under human control. Such reporting would mirror the transparency measures of classic arms control (for example, the UN Register of Conventional Arms). Analysts note that establishing standards for information sharing and notifications about AI-enabled systems can make inadvertent conflict less likely by reducing surprises. Over time, a series of small confidence-building steps, such as political declarations, data exchanges and joint studies, can cumulate into shared norms.

Several concrete CBM ideas have been floated by experts (Puscas 2022; Scharre and Lamberth 2022; Horowitz and Kahn 2021). For example, states could convene technical working groups to elaborate common definitions and standards for AI safety, so that everyone measures reliability by similar yardsticks. They could agree to incident notification mechanisms: if an AI-related mishap with cross-border implications occurs, affected states inform others through a secure channel. A UNIDIR study suggests starting with politically easier steps (unilateral or bilateral measures) and gradually institutionalizing them multilaterally (Puscas 2022). Early CBMs might be as simple as publishing national AI strategies or inviting foreign experts to observe a demo of a defensive AI system. Such moves let states “test the water” of cooperation at their own comfort level. Over time, if these actions reassure others, states may feel more confident and pursue formal agreements. In the end, confidence building is about signalling good faith, demonstrating through deeds that one seeks to avoid destabilization. With AI, where mistrust and fear of the unknown run high, CBMs are not just a trust-building exercise but a risk-mitigation necessity. They operationalize transparency and accountability, helping to ensure that the race for AI does not outrun the cultivation of confidence.

Recommendations

Building on the analysis above, this brief makes the following actionable recommendations to embed trust and trustworthiness *by design* into AI's military and security applications. These measures are aimed at policy makers and stakeholders seeking practical steps to enhance global security through cooperative governance of AI.

Establish Voluntary AI Transparency and Reporting Mechanisms

Nations should institute voluntary confidence-building measures that mirror arms-control transparency practices for AI. For example, states could agree to regular reporting on their military AI doctrines, the types of AI-enabled systems they are developing or deploying, and the safety measures in place. An international registry (perhaps under UN auspices) could be created where countries submit annual reports on AI in armed forces, including incidents or near-misses involving AI (Horowitz and Scharre 2021; Horowitz and Kahn 2021). Such voluntary exchanges will demystify countries' AI activities and reassure others that there are no secret destabilizing programs.

By sharing this information, states demonstrate a commitment to responsible use, addressing the fear of the unknown. Analysts have noted that creating standards for information sharing and notifications about AI systems can markedly lessen the risk of inadvertent conflict by clarifying intentions. Voluntary reporting is a flexible, non-binding approach, lowering political barriers to participation, but over time it can build confidence and potentially pave the way to more formalized agreements. International organizations and neutral third parties (such as the International Committee of the Red Cross or academic consortia) could host the data and provide assessments, adding credibility. Transparency is contagious: as more countries participate, pressure will grow on holdouts to show they have nothing to hide, thereby raising the global norm of openness in military AI.

Adopt and Internationally Endorse Human Agency Impact Assessments and Ensure Norm of Human Control

In 2019, the Canadian government released the Directive on Automated Decision-Making, which included the Algorithmic Impact Assessment — a questionnaire designed to reduce risks and mitigate potential negative impacts when AI technologies are used. A similar impact assessment should be developed to address how AI tools and systems are impacting human decision making. In military AI applications, due to the use of AI decision-support systems, for example, it is increasingly more helpful to consider impacts on human agency as AI tools shape decision making (Bode 2025). To prevent automation bias and preserve legal and moral responsibility, any AI that influences the use of force should undergo a human agency impact assessment. The assessment could map task allocation, operator workload, failure modes, escalation risks and explicit authorities to intervene or abort.

Crucially, the principle of maintaining human control over decisions to use force must be unequivocally upheld. All nations, and any emergent norms or declarations, should formally endorse that critical functions in weapons systems (especially the application of lethal force) remain under direct human control and judgment. This can be operationalized through standards or protocols that require a human operator's affirmative decision for any AI-identified target engagement, and robust oversight of autonomous systems (Lindelauf and Meerveld 2025). To put this into practice, military organizations worldwide should develop an explicit doctrine that aligns with national policies for human supervision of AI — for example, requiring that autonomous systems in weapons roles are always paired with a human commander who can intervene or abort. Internationally, states could incorporate these standards into their rules of engagement and share those policies as best practices. Multilaterally, a consensus could be built around updating Article 36 weapons reviews (required by Additional Protocol I of the Geneva Conventions) to specifically ensure any AI-based weapon is designed and tested to allow effective human control. Such standards not only prevent unethical outcomes but also build interstate trust: rivals are less anxious about each other's AI if they know humans are firmly in control.

A useful step would be a joint statement, perhaps at the UN General Assembly, affirming the human-in-control norm. Even without a binding treaty, a political affirmation by a broad group of states would set expectations and guide military procurement. This should be supplemented by training and simulation exercises that reinforce human judgment in AI-augmented decision making, to prevent overreliance on automation. Additionally, mechanisms for accountability should be part of the standard; if an AI-related incident occurs, the state must investigate and a human commander is accountable, ensuring there is always a responsible human agent.

Promote Regional AI Security Dialogues and Risk-Reduction Protocols

While global norms are crucial, many security dynamics play out at the regional level. It is recommended that regional organizations and fora develop tailored strategies for AI governance that complement global efforts. For instance, in Europe, the Organization for Security and Cooperation in Europe could integrate AI into its existing confidence- and security-building measures tool kit, expanding data exchanges or inspection regimes to cover certain autonomous systems. The European Union, through its peace and security bodies, might facilitate regional agreements on the responsible use of AI by member states' militaries, building on the European Union's own AI Act (which already prohibits some harmful AI applications) (Romansky 2025). In the Asia-Pacific, the Association of Southeast Asian Nations (ASEAN) Regional Forum or the East Asia Summit could host workshops on AI in defence to increase transparency among regional rivals (for example, dialogues involving China, India, Japan, the Republic of Korea and ASEAN states on naval autonomous systems in the South China Sea or on the subcontinent). Indeed, UNIDIR and REAIM have hosted these types of dialogues. These regional discussions can address specific flashpoints where AI might be deployed, crafting localized CBMs, such as an agreement among certain Asian powers not to deploy autonomous naval vehicles along disputed borders, or an understanding in the Middle East to notify neighbours when deploying AI-enabled surveillance along frontiers to avoid misinterpretation.

Conclusion

The progressive integration of AI into military affairs requires greater trust building. The answer lies in cultivating trust by design at multiple levels, in the technology, in the humans using that technology and among the nations setting the rules of the game. That cultivation process is now under way, but it must accelerate. This brief has highlighted that trust and trustworthiness are not automatic; they result from deliberate choices in policy, diplomacy and design of technologies. Multilateral efforts are converging on key themes: transparency, human control and inclusive cooperation. The task ahead is to translate principles into practice, through concrete measures such as the ones recommended here, and to do so with urgency.

Ultimately, trust-by-design frameworks cannot solve the issues of strategic deception or macro-political distrust. Still, by focusing on confidence-building measures and exchanges of information among various states, some of the proposed efforts are critical to lowering the temperature and developing ways to build shared standards and norms. As Friedman warned and Ambassador Shen echoed, in their own ways, without common standards and mutual confidence, an AI-driven world could become unmanageably dangerous. It is fitting that middle powers and a broad coalition of states are stepping up to guide those choices, reminding the superpowers that international security is a shared responsibility. Trust is both the ingredient and the outcome of their collaborative leadership. Through confidence-building measures, dialogue and assistance, we can ensure that AI systems are deployed with transparency and restraint, not in destabilizing secrecy. Admittedly, geopolitical realities will make the path rocky, but implementing trust by design now is the surest way to manage military AI responsibly and reduce escalation risk.

Works Cited

- Abraham, Yuval. 2024. "‘Lavender’: The AI machine directing Israel’s bombing spree in Gaza." *+972Magazine*, April 3. www.972mag.com/lavender-ai-israeli-army-gaza/.
- Bode, Ingvild. 2025. *Human-Machine Interaction and Human Agency in the Military Domain*. CIGI Policy Brief No. 193. Waterloo, ON: CIGI. www.cigionline.org/publications/human-machine-interaction-and-human-agency-in-the-military-domain/.
- Chaulagain, Susmita. 2025. "UN experts call for regulations to ensure AI developments respect human rights." *Jurist*, April 6. www.jurist.org/news/2025/04/un-experts-calls-for-regulations-to-ensure-ai-developments-respect-human-rights/.
- Friedman, Thomas. 2025. "What I’m Hearing in China This Week About Our Shared Future." Opinion. *The New York Times*, March 25. www.nytimes.com/2025/03/25/opinion/trump-china-ai.html.
- Gillespie, Nicole, Steve Lockey, Tabi Ward, Alexandria Macdade and Gerard Hassed. 2025. *Trust, attitudes and use of artificial intelligence: A global study 2025*. The University of Melbourne and KPMG. <https://doi.org/10.26188/28822919>.
- Horowitz, Michael C. and Lauren Kahn. 2021. "Leading in Artificial Intelligence through Confidence Building Measures." *The Washington Quarterly* 44 (4): 91–106. <https://doi.org/10.1080/0163660X.2021.2018794>.
- Horowitz, Michael C. and Paul Scharre. 2021. *AI and International Stability: Risks and Confidence-Building Measures*. Center for a New American Security. January. www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures.
- Klingbeil, Artur, Cassandra Grützner and Philipp Schreck. 2024. "Trust and reliance on AI — An experimental study on the extent and costs of overreliance on AI." *Computers in Human Behavior* 160, 108352. <https://doi.org/10.1016/j.chb.2024.108352>.
- Lindelau, Roy and Herwin Meerveld. 2025. Building Trust in Military AI Starts with Opening the Black Box. *War on the Rocks*, August 12. <https://warontherocks.com/2025/08/building-trust-in-military-ai-starts-with-opening-the-black-box/>.
- Marijan, Branka. 2025. *Through a Glass Darkly: Transparency and Military AI Systems*. CIGI Paper No. 315. Waterloo, ON: CIGI. www.cigionline.org/publications/through-a-glass-darkly-transparency-and-military-ai-systems/.
- Merchán-Cruz, Emmanuel A., Ioseb Gabelaia, Mihails Savrasovs, Mark F. Hansen, Shwe Soe, Ricardo G. Rodriguez-Cañizo and Gerardo Aragón-Camarasa. 2025. "Trust by Design: An Ethical Framework for Collaborative Intelligence Systems in Industry 5.0." *Electronics* 14 (10): 1952. <https://doi.org/10.3390/electronics14101952>.
- Puscas, Ioana. 2022. "Confidence-Building Measures for Artificial Intelligence: A Framing Paper." Geneva, Switzerland: UNIDIR. https://unidir.org/wp-content/uploads/2023/05/Confidence-Building_Final.pdf.
- Robins-Early, Nick. 2024. "AI’s ‘Oppenheimer moment’: autonomous weapons enter the battlefield." *The Guardian*, July 4. www.theguardian.com/technology/article/2024/jul/14/ais-oppenheimer-moment-autonomous-weapons-enter-the-battlefield.
- Roff, Heather M. and David Danks. 2018. "‘Trust but Verify’: The Difficulty of Trusting Autonomous Weapon Systems." *Journal of Military Ethics* 17 (1): 2–20. <https://doi.org/10.1080/15027570.2018.1481907>.
- Romansky, Sofia. 2025. "Lessons from the EU on Confidence-building Measures Around Artificial Intelligence in the Military Domain." Stockholm International Peace Research Institute. May. www.sipri.org/publications/2025/eu-non-proliferation-and-disarmament-papers/lessons-eu-confidence-building-measures-around-artificial-intelligence-military-domain.
- Scharre, Paul and Megan Lamberth. 2022. *Artificial Intelligence and Arms Control*. Center for a New American Security. October. www.cnas.org/publications/reports/artificial-intelligence-and-arms-control.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel **Aaron Shull**
Director, Programs **Dianna English**
Senior Program Manager **Jenny Thiel**
Manager, Publications **Jennifer Goyder**
Graphic Designer **Sepideh Shomali**

Copyright © 2025 by the Centre for International Governance Innovation

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.



The text of this work is licensed under CC BY 4.0. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

For reuse or distribution, please include this copyright notice. This work may contain content (including but not limited to graphics, charts and photographs) used or reproduced under licence or with permission from third parties. Permission to reproduce this content must be obtained from third parties directly.

Centre for International Governance Innovation and CIGI are registered trademarks.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

