AISE MARKERS SERIES

Benchmark I: Governance

Insights from the Global Conference on AI, Security and Ethics 2025

YASMIN AFINA · JAN HENDRIK MANNSPERGER

1. Introduction

1.1. Context

On 27–28 March 2025, UNIDIR organized its inaugural Global Conference on Artificial Intelligence, Security and Ethics (AISE25), hosted in the Palais des Nations, Geneva. Led by UNIDIR's Security and Technology Programme, the conference provided an agile response to rapid advances in artificial intelligence (AI), which have put this technology at the forefront of today's global policy discussions. AISE25 was held as policymakers and regulators worldwide increasingly recognized the urgency of developing shared understandings, norms and regulations that can transcend national borders and individual interests, including in the context of peace and security.

The conference sought to provide a unique forum for engagement between the multilateral ecosystem and the wider multi-stakeholder community, including academic experts, civil society organizations, industry representatives and research laboratories interested in the governance of AI in peace and security. By jointly analysing and addressing the complex implications of AI for national, regional and global security and resilience, AISE25 enriched dialogue between participants and exposed them to the latest research in the field. This opportunity to exchange and consolidate views on AI in the military domain was timely, with the United Nations General Assembly having requested the views of Member States and other stakeholders as a means of informing discussions during its Eightieth Session, in September 2025 – the deadline for which came just weeks after the conference.[1]

The conference programme was designed to build on the work undertaken as part of UNIDIR's Roundtable for AI, Security and Ethics (RAISE), a multi-year project on multi-stakeholder engagement in this space launched with the support of Microsoft.[2] Specifically, the conference's agenda was primarily organized around the six priority themes identified at the inaugural edition of RAISE, which took place in Bellagio, Italy, in March 2024:[3]

1. Knowledge and capacity-building
2. Trust-building
3. The human element
4. Data practices
5. Life cycle management
6. Addressing destabilization

Combining a series of panel discussions, presentations in the form of thematic deep-dives and lightning talks, as well as a poster exhibition, AISE25 provided a timely platform, open to all, to jointly consider and elaborate on each of these six priority themes while promoting meaningful dialogue and cooperation.

Ahead of the second edition of the AISE, in June 2026, a series of three reports – the first of the AISE Markers series – takes stock of the key takeaways from AISE25 to provide an initial basis and scaffolding for AISE26. By acting as a bridge between editions of AISE, the AISE Markers series will ensure that each conference is built on solid ground and constitutes a natural evolution from the discussions held in the previous conference.

This first report gives a structured account of where the conversation on governance stood at the time of AISE25. It provides an overview of shared understandings and possible areas of tension and identifies areas that remain unresolved and may subsequently serve as a baseline for AISE26. Accompanying reports will cover the state of technology and use cases.

1.2. The governance imperative: The need for structured engagement and operationalization pathways

AISE25 convened at a moment of momentum in the governance of AI in security and defence, as reflected in a shared sense of need and urgency for structured engagement on these issues. While there is recognition of the opportunities that AI technologies may

1 General Assembly, resolution 79/239, "Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security", 24 December 2024, https://docs.un.org/A/RES/79/239.

2 UNIDIR, "RAISE: The Roundtable for AI, Security and Ethics", https://unidir.org/raise/.

3 Y. Afina and G. Persi Paoli, *Governance of Artificial Intelligence in the Military Domain: A Multi-Stakeholder Perspective on Priority Areas* (Geneva: UNIDIR, 2024), https://unidir.org/publication/governance-of-artificial-intelligence-in-the-military-domain-a-multi-stakeholder-perspective-on-priority-areas/.

bring for international peace and security, a host of concerns were shared at the conference that highlighted the need for dialogue, mutual understanding and collective action.

The stakes were set from the outset by the United Nations Secretary-General in his message to the conference. With recent conflicts being considered as testing grounds for military AI, concerns have arisen about compliance with international law and civilian harm. As the conversation has now come to the United Nations, the Secretary-General underscored the need to turn commitment into action with human rights, human dignity and human agency at the core of an "AI for good".[4] Subsequent interventions further emphasized the need for such discussions amid the acknowledgment that the deployment and use of AI in military and security contexts are no longer hypothetical: the question is not whether, but precisely how these technologies are to be used.

The imperative for governance, however, does not necessarily equate to restrictions only. As reflected throughout the conference, governance serves as infrastructure, architecture and a template for security and stability, rather than as a brake on capability. That is, governance efforts revolve around setting the preconditions for security, predictability, trust, peace and prosperity.

In parallel, the AI governance paradox further stresses the importance of the discussions the conference has facilitated: recognizing that regulation may, sometimes, lag behind technology makes it essential that, through on-going dialogue, the policy and technical communities develop, collectively, tools for effective governance. To this end, historical experience highlights the value of a four-point, holistic and mutually reinforcing response: normative frameworks, technical standards, capacity-building and inclusive multilateral platforms.[5]

Against this backdrop, AISE25 took place at an inflection point: amid a cluster of institutional developments, particularly within the United Nations, 2025 was characterized as "another key year" with respect to AI in the military domain.[6] Specifically, the General Assembly adopted resolution 79/239 in December 2024, the first specifically on AI in the military domain.[7] This resolution is particularly considered as a landmark in the light of its scope, which extends beyond lethal autonomous weapon systems (LAWS) to encompass a host of applications, ranging from command and control, decision support and intelligence, via logistics support to training and cyber operations. The resolution further mandates a report from the Secretary-General drawing on states' submission of views on this issue.[8] More broadly, the Pact for the Future commits states to assess AI risks in military applications. Taken together, these developments attest to the Secretary-General's assertion: the conversation has come to the United Nations, offering an inclusive pathway for discussions open to all Member States.

---

4 "UN Secretary General's message to the inaugural Global Conference on AI, Security and Ethics", UNIDIR, 27 March 2025, https://unidir.org/un-secretary-generals-message-inaugural-global-conference-ai-security-ethics/.

5 As highlighted by Nur Sulyna Abdullah (International Telecommunication Union, ITU) in day 1's opening panel, these reflections draw on the ITU's experience in navigating successive waves of science and technological innovation since 1865, from the telegraph that once constituted a groundbreaking technology to, today, generative AI.

6 As noted by Izumi Nakamitsu (United Nations Office for Disarmament Affairs) in day 1's opening panel.

7 General Assembly, resolution 79/239.

8 Since AISE25, the Secretary-General has issued his report: General Assembly, "Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security", Report of the Secretary-General, A/80/78, 5 June 2025, https://docs.un.org/A/80/78.

2. National approaches to the governance of AI, security and ethics

States are developing approaches to the governance of AI in defence at speed but from divergent starting points. AISE25 offered four national case studies – the Netherlands, the United Arab Emirates (UAE), Singapore and China – each representing a distinct approach to governance.

2.1. The Netherlands: Building a defence AI strategy

In developing its 2023 defence AI strategy, the Netherlands proceeded from the recognition that no universal blueprint exists for integrating AI into defence.[9] National and regional context necessarily shapes the choices available to any state.

A defining feature of the Dutch approach is its deliberately broad scope: it does not adopt a narrow understanding of AI as the primary frame; instead, the strategy situates AI within the wider fields of data science and data governance. Analytics techniques beyond AI may in some contexts indeed offer more suitable or implementable solutions: when access to or availability of data is limited, or the complexity of the solution is too great, other techniques may be more appropriate. For instance, the so-called Goalkeeper Close-in Weapon System (CIWS) on Dutch Navy vessels, which has existed for almost 25 years, can target incoming missiles and operates largely autonomously; but it runs on an optimization algorithm, not an AI algorithm. In that specific context, it provides more reliable functionality than a more elaborate AI solution would, underscoring that AI is not the solution for every context.

The defence AI strategy identifies four key enablers: powerful information technology (IT) capabilities; data governance; knowledge and skills; and a data-driven culture.

The first of these, IT capabilities, underpins the other enablers. The Netherlands does not treat a requirement for robust IT infrastructure in isolation but as part of a broader digital transformation encompassing cloud architecture, cybersecurity and data systems. In this area, a key structural concern is digital sovereignty: when critical infrastructure is predominantly owned by private technology companies, the degree of sovereign control available to a defence ministry is inherently constrained.

Data governance is the foundational, empowering part of AI, and accounts for roughly 80 per cent of the effort required to get an AI system working. Roles, responsibilities and operating principles for governing data are therefore a precondition for moving to AI. The quality and availability of data ultimately determine the value of data science and AI applications. AI algorithms also operate in specific contexts (i.e., land, maritime, air, space, cyber) and data-governance mechanisms need to align with those commands and units. The Netherlands is currently implementing a data-governance model based on a central framework, with responsibility decentralized towards commands.

9 See: Ministry of Defence of the Kingdom of the Netherlands, Data Science and AI Strategy 2023-2027 (Defensie Strategie Data Science en AI 2023-2027) (2023), https://www.rijksoverheid.nl/documenten/2023/05/31/defensie-strategie-data-science-en-artificiele-intelligentie-2023-2027.

Data literacy is another key pillar of integration. Monitoring and evaluation of AI-driven systems will increasingly become important tasks for armed forces. As military personnel tend to serve for long periods, they need to be trained accordingly. Operators need to be able to assess the quality of data and outputs and to understand the implications of how AI is speeding up intelligence processing and decision-making. This also encompasses research and development, enabling AI to be developed responsibly. Thorough testing is needed to assess whether an application acts as designed and is suited for deployment in a specific context – aiming for safety, reliability and transparency. Accordingly, the Netherlands has also invested heavily in a Centre of Excellence for data science, and it is very important to have personnel with doctorates working within the military domain conducting research on AI applications.

The most challenging enabler is institutional culture. Shifting military decision-making away from reliance on experience and seniority towards data-informed approaches has required deliberate change management. This has included simulation exercises in which personnel compare decisions made independently with those made using AI assistance.

Among areas of application of defence AI, the Netherlands prioritizes logistics and business operations as an entry point, assessing them to be the domains with the most mature data-governance infrastructure through existing enterprise resource planning (ERP) systems. Progress to the more complex domains of autonomous systems, intelligence analysis and military decision-making will follow.[10]

2.2. The United Arab Emirates: Strategic partnership and knowledge co-development

A central principle of the approach taken by the United Arab Emirates to technology governance is the distinction between transactional procurement and strategic partnership. Rather than acquiring technology through purchase and applying safeguards after the fact, the UAE has pursued deep collaborative relationships with foreign partners involving joint knowledge development, shared intellectual property (IP) and embedded transparency mechanisms. The rationale is that transactional approaches, however well-structured, do not in themselves generate the institutional culture or systemic accountability that responsible technology usage requires; strategic partnerships do.

This model is illustrated by the UAE's space programme, where collaboration with partners from the Republic of Korea on its first remote sensing satellites involved mutual exchange of background IP and the joint generation of foreground IP. This not only produced a technical outcome but also aligned engineering cultures, which has sustained the partnership over time. Similar frameworks governed the UAE's deep space mission, developed with the University of Colorado Boulder in the United States, and its nuclear programme, implemented through a consortium involving the Republic of Korea and the United States with extensive transparency and verification mechanisms.

The UAE situates this partnership model within a broader posture of deliberate non-alignment in technology partnerships. Given its historical role as a trade hub and its contemporary relationships spanning across technology ecosystems, the UAE has articulated a position

10 As noted by Jeroen van der Vlugt (Netherlands Ministry of Defence) in the deep-dive on "Building a Defence AI Strategy: The Dutch Approach" on day 1.

of engaging multiple partners across geopolitical lines, rather than consolidating within a single bloc. Three red lines cannot be crossed in these engagements: national sovereignty, institutional credibility and mutual trust with partners. Within those constraints, the UAE maintains parallel cooperation arrangements, including structural protections for each partner's requirements.

Assessments of the threat environment also inform the UAE's approach. The reported use of converted civilian technologies by non-state actors in the Red Sea to disrupt global maritime trade is a concrete illustration of how advanced and emerging technologies can be weaponized outside conventional state frameworks. This has implications for how governance approaches to AI and dual-use technologies should be designed.

More broadly, the UAE frames its AI strategy within a civilian development paradigm: it identifies healthcare, education and social services as primary drivers, with security considerations secondary. Strategic foresight is a key approach to these challenges: the UAE identifies where technology is reshaping competitive landscapes and positions itself accordingly, rather than following incremental conventional pathways.[11]

2.3. Singapore: From national principles to regional norms

Singapore's approach to the governance of military AI proceeds from the state-centric framing that the objective is to survive and thrive within the international system. In the context of military AI, this means developing the capability to make deployment and governance decisions consistent with national interests, while engaging effectively in the development of international norms and regulations.

Singapore situates military AI governance within its broader national AI strategy, which seeks to enable AI adoption across sectors while managing associated risks. Singapore's national principles for AI in the military domain are comprised of the 3R1S framework: Responsible, Reliable, Robust and Safe. The development of this framework was the product of extensive multi-stakeholder consultation involving defence technologists, military planners, international law experts and policy professionals. The framework governs the full development and deployment life cycle of AI-enabled military systems.

At the regional level, Singapore emphasizes the significance of cooperation on AI governance, taking on an active convening role. Its co-hosting of Asian regional consultations in February 2024 revealed a consistent finding: states across the region treat national-level capacity-building as a priority first step, pursued in parallel with engagement in regional forums. Within the Association of Southeast Asian Nations (ASEAN), a joint statement on defence AI cooperation issued by the ASEAN Defence Ministers' Meeting in February 2025 that commits member states to information exchange and sharing of best practices is noted as meaningful progress towards common regional approaches.[12]

A substantive concern running through Singapore's approach is what it characterizes as a risk-only framing in many capacity-building efforts. Singapore assesses approaches that concentrate exclusively on risk mitigation, and

11 As noted by H.E. Omran Sharaf (Assistant Foreign Minister for Advanced Science and Technology, United Arab Emirates) in his Fireside Chat on day 1.

12 ASEAN, "Joint Statement by the ASEAN Defence Ministers on Cooperation in the Field of Artificial Intelligence in the Defence Sector", 26 February 2025, https://asean.org/joint-statement-by-the-asean-defence-ministerial-on-cooperation-in-the-field-of-artificial-intelligence-in-the-defence-sector/.

in some cases trend towards calls for capability bans as leaving states poorly positioned to make informed, sovereign decisions about emerging technologies. Effective capacity-building, Singapore argues, must equip states to evaluate AI across both its risks and its opportunities, and to do so on the basis of independently developed knowledge and human capital, rather than externally supplied conclusions. Sovereignty, in this framing, encompasses the epistemic capacity to assess technology on the state's own terms.

A final and operationally significant observation concerns the intended beneficiaries of capacity-building. Singapore identifies policymakers, military commanders and diplomats – rather than technical specialists – as the primary audience. It also notes a significant gap between the complexity of technical, legal and ethical material and the forms in which it reaches decision makers. The practical implication is that subject-matter experts bear a responsibility to translate specialist knowledge into forms that can be operationalized in national contexts and are applicable in international settings. Terminological inconsistency and conceptual misunderstanding across delegations are identified as concrete obstacles to the development of norms, with direct consequences for peace and security.[13]

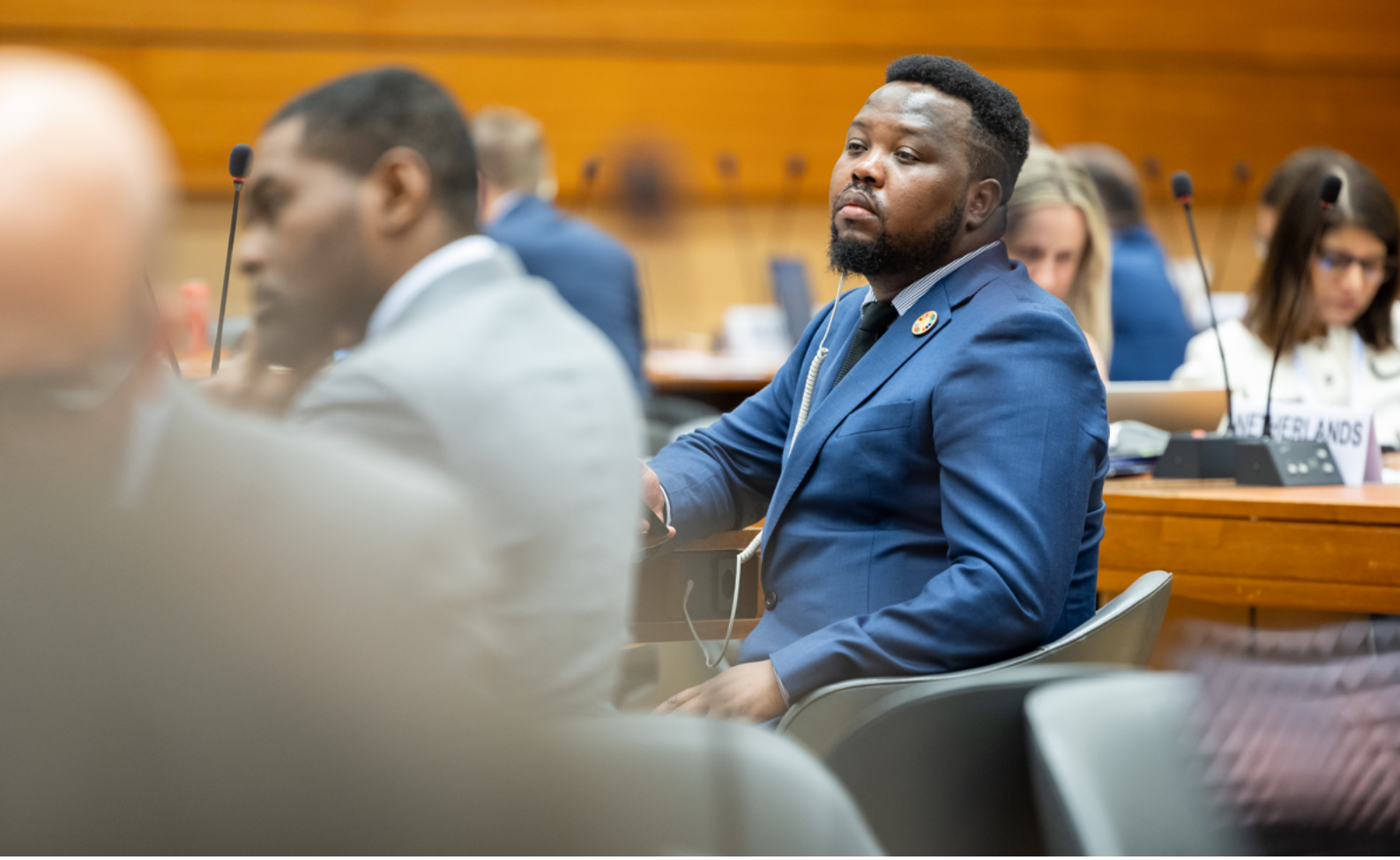
2.4. China: Trust, fragmentation and the case for universal AI governance

China sees the central challenge of global AI governance as one of trust. Trust is identified as both a scarce resource in the current international environment, but necessary to tackle challenges posed by global AI development. Without trust between major AI powers, each country will proceed to developing its own AI systems in isolation and without shared norms, mutual transparency or collective governance capacity. The result will be technological feudalism and risks at a civilizational scale. China reiterates the warning among intellectuals that humanity must build trust among itself before developing truly superintelligent AI agents, and that losing trust with those outside one's own bloc leaves all parties vulnerable to AI systems that escape meaningful human governance.

From China's perspective, current trust deficits have identifiable structural causes. Export control regimes are perceived in Beijing as containment of China's development in advanced technologies. Reported pressure on third countries to restrict technology transfers reinforces this interpretation. Export controls are frequently justified on the grounds that any technology transfer could enhance the military capabilities of the importing countries. However, national security concerns, if left unchallenged, will only deepen the trust deficit.

The consequences of continued polarization extend beyond bilateral relationships to multilateral and international governance mechanisms, processes and initiatives. These include discussions within the framework of the Convention on Certain Conventional Weapons (CCW) Group of Governmental Experts on LAWS, the Bletchley process, and the Conference on Disarmament. Yet, by severing the shared technological and normative ground on which they depend, parallel AI ecosystems that divide states and regions would undermine the effectiveness of these frameworks. Fragmentation, in this view, is not a stable equilibrium but an erosion of the international community's collective capacity to govern AI in the common interest.

13 As noted by Pak Shun Ng (Ministry of Defence, Singapore) in the panel on "Global Commission on Responsible AI in the Military Domain" on day 1.



China's constructive position is organized around two principles drawn from President Xi Jinping's Global AI Governance Initiative and reflected in a working paper submitted by China to the CCW.[14] The first, AI for Good, holds that AI technologies should serve humanity broadly, rather than entrench military superiority for any single power or undermine strategic stability: tiered regulation of military AI applications is identified as a necessary instrument towards this end. The second, AI for All, addresses the development dimension: growing capability gaps between states are characterized not only as an economic or technological concern but as a security concern in their own right, on the grounds that development gaps generate security gaps. These may, in turn, produce regional instability and risk contributing to armed conflict. Ensuring broad access to AI's benefits is therefore a prerequisite for sustainable global security.[15]

14 Working Paper of the People's Republic of China on Lethal Autonomous Weapons Systems (2022), https://documents.unoda.org/wp-content/uploads/2022/07/Working-Paper-of-the-Peoples-Republic-of-China-on-Lethal-Autonomous-Weapons-Systems%EF%BC%88English%EF%BC%89.pdf.

15 As noted by Ambassador Shen Jian (Ambassador Extraordinary and Plenipotentiary (Disarmament) and Deputy Permanent Representative, China) in the panel on "Trust-Building" on day 1.

3. International efforts

The international policy landscape for the governance of AI in security and defence is in flux and at a critical juncture, with many shared concerns about fragmentation and about the operationalization of applicable norms and principles. Beyond the United Nations, many initiatives have emerged, with particular attention being given to the Responsible AI in the Military Domain (REAIM) initiative and the work of the Global Commission on Responsible AI in the Military Domain (GC REAIM). Against this backdrop of mushrooming dedicated initiatives, AISE25 also shed light on the importance of considering the application of existing international law throughout the life cycle of military AI technologies, particularly in the context of international humanitarian law (IHL) and international human rights law (IHRL).

3.1. Military AI in the United Nations: What resolution 79/239 clarifies and what remains uncertain

While Member States have been grappling with the issue of LAWS for over a decade within the context of the CCW , including in the form of a Group of Governmental Experts (GGE),[16] attention to other applications of AI in the context of international peace and security has remained limited and sporadic, if not restricted.[17] Resolution 79/239 thus marks a significant milestone, by calling for states and the wider multi-stakeholder community to report their views and by explicitly broadening the scope of submissions to "areas other than lethal autonomous weapons systems".[18]

Views on the way ahead will form a key component of these submissions, with an invitation for states to define the most appropriate format for future discussions on this issue. Taking into account past and on-going models and mechanisms for deliberations in other security and technological fields (including in the format of GGEs, open-ended working groups, open-ended technical expert groups and independent scientific panels), future deliberations on military AI and its implications for international peace and security will need to account for both the governance and the technical dimensions.

This call for views by states – and the wider multi-stakeholder community – was intended to inform a report by the United Nations Secretary-General, as mandated by resolution 79/239, which was to be used as a basis for a follow-up resolution on this issue.[19] All possible options for future discussions within the United Nations offer an opportunity for all Member States (and, as appropriate, the wider multi-stakeholder community) to participate.

---

16 These discussions were catalysed in particular by the 2013 report of the late Christof Heyns, Special Rapporteur on extrajudicial, summary or arbitrary executions, on lethal autonomous robotics: Human Rights Council, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, A/HRC/23/47, 9 April. 2013, https://docs.un.org/A/HRC/23/47.

17 In 2024, much attention was given to two General Assembly resolutions on AI: resolution 78/265 on sustainable development, 1 March 2024, https://docs.un.org/A/RES/78/265, and resolution 78/311 on capacity-building, 1 July 2024, https://docs.un.org/A/RES/78/311. However, both purposefully exclude the military domain from their scope. See preamble 6 of resolution 78/265 and preamble 6 of resolution 78/311.

18 General Assembly, resolution 79/239, operative paragraph 7.

19 Since then, in mid-2025 the Secretary-General published his report on AI in the military domain, A/80/78. The General Assembly subsequently adopted, in its 80th session, resolution 80/58, "Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security", 1 December 2025, https://docs.un.org/A/RES/80/58.

This is particularly important, considering that conversations should not be exclusively led by states that are in possession of advanced technologies.

3.2. The REAIM initiative: An incubator and its limits

Developments within the United Nations are unfolding in parallel to on-going state-led initiatives. These include the REAIM initiative, which was catalysed by its first summit, hosted by the Netherlands in The Hague in February 2023. Following its second edition, hosted by the Republic of Korea in Seoul in September 2024, the initiative is generally presented as providing a platform for reflection on the concept of responsibility in the context of AI in the military domain. Beyond avoiding misuse, responsibility is also presented as proactively ensuring that AI is developed and deployed in ways that prioritize safety, lawfulness and international alignment amongst States and stakeholders.[20] Achieving the responsible development and deployment of AI in the military domain is, however, acknowledged as an issue that cannot be managed by states only – it requires steps and measures that depend on actors involved throughout the technology's life cycle. This observation underpins the multi-stakeholder nature of the REAIM Summits, which include sessions led by representatives of the private sector, civil society and academia – in addition to the initiative's political track with the adoption, by a number of invited states, of an outcome document at the conclusion of each summit.

While REAIM is presented as an incubator for ideas and, eventually, "gradual norm development",[21] without prejudice to its future trajectory, concerns arise with respect to participation and representation at REAIM. Its state-led nature, sitting outside the United Nations, means that state representation is not universal, raising concerns about inclusivity and representability.[22]

3.3. The Global Commission on Responsible AI in the Military Domain

The Global Commission on Responsible AI in the Military Domain was established by the Ministry of Foreign Affairs of the Kingdom of the Netherlands in early 2023 during the inaugural REAIM Summit, with a mandate to formulate strategic guidance for the international community. GC REAIM has an interdisciplinary and cross-regional membership to draw on, consisting of 17 commissioners and 31 members of the Expert Advisory Group (all serving in their personal capacity). The commission was established with the view to promoting mutual understanding among the communities involved in this space, in addition to creating new avenues for cooperation to support norm development and policy coherence. Acknowledging the risks that these technologies may introduce or

20 As noted by Ambassador Song Si-jin (Permanent Representative of the Republic of Korea to the Conference on Disarmament) in the closing panel of day 2.

21 Ibid.

22 As noted by Vadim Kozyulin (Russian Diplomatic Academy) in day 2's panel on the human element. Furthermore, after AISE25, the third REAIM Summit took place in Spain in February 2026, with a series of regional consultations in its lead-up. UNIDIR's report on the 2025 regional consultations identifies a number of perceived challenges, from states, surrounding REAIM and its outcome documents – one of which specifically relates to concerns surrounding the long-term sustainability of a non-United Nations forum to provide space for interstate deliberations. See Yasmin Afina, *The Global Prism of Military AI Governance: Reflections from the 2025 Regional Consultations on Responsible AI in the Military Domain* (Geneva: UNIDIR, 2026), https://unidir.org/publication/the-global-prism-of-military-ai-governance-reflections-from-the-2025-regional-consultations-on-responsible-ai-in-the-military-domain/.

exacerbate, it was also important for the commission to consider the opportunities that AI may offer to the military domain, ranging from supporting logistics and productivity to command and control, as well as decision-support systems.

The work of GC REAIM was divided into four workstreams: technological foundations; implications for international peace, security and stability; decision-making and responsibility; and governance and regulation.[23]

Technological foundations

This workstream sought to develop a comprehensive taxonomy that not only captures the technical characteristics of AI and its different fields and subfields (e.g., machine learning and deep learning), but also the different use cases of AI in the military domain. Additionally, the workstream explored a three-pronged contextualization framework to support the commission's thinking on the operationalization of responsible AI in the military domain: (a) the domain of operation (e.g., land, air, sea and cyberspace); (b) the spectrum of conflict (i.e., peacetime, wartime or grey zone operations); and (c) the type of military activity (e.g., offensive operation, defensive operation, support operation, kinetic and non-kinetic).

International peace, security and stability

There is a general recognition of the (extreme) implications that AI has for international peace, security and stability. This is partly due to the unique characteristics of AI technologies, particularly in the light of their inherently dual-use nature and their subsequent scalability, their potential to be repurposed, and their widespread distribution within military contexts. The workstream looked into the convergence of these technologies with weapons of mass destruction (WMD), including in the context of AI integration into nuclear command and control, as well as the perceived concerns over large language models that may facilitate WMD proliferation. Other issues that may have implications for international peace, security and stability include the prospect of a military AI arms race and the reduction in thresholds leading to the use of force.

Decision-making and responsibility

This workstream looked into the critical themes surrounding decision-making and responsibility in the context of AI in the military domain. The issues covered include the extent to which AI systems may undermine the conditions to establish human responsibility and the implications of integrating AI agents into military decision-making processes. Consequently, beyond looking into responsibility in decision-making, the workstream also looked into the conceptualizing of what responsible innovation and development concretely mean and what operationalization would entail.

Governance and regulation

A key principle that grounds the work of the GC REAIM is the understanding that the governance of AI in the military domain must be founded in existing international law. While the development, deployment and use of these technologies may raise a number of challenges and issues, international law already applies – thus addressing the assumption that governance efforts are starting "from scratch". The commission also noted the importance of applying, holistically, all applicable branches of public international law. While there has been an emphasis on international humanitarian law in existing discussions, other

23 Since the convening of AISE25, GC REAIM has issued its Strategic Guidance Report, which reflects the views, independent judgment and deliberations of the commission's chair and commissioners. See Global Commission on Responsible Artificial Intelligence in the Military Domain (GC REAIM), *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain* (The Hague: GC REAIM, September 2025), https://hcss.nl/wp-content/uploads/2025/09/GC-REAIM-Strategic-Guidance-Report-Final-WEB.pdf.

branches must also be considered, including international human rights law, *jus ad bellum* and environmental law, in addition to the procedural dimension of the international legal system. On this basis, the workstream looked at a host of issues that touch upon governance and regulations, including possible gaps that may potentially require the formulation of new norms, as well as the question of implementation and enforcement.

The commission's work has not only drawn on its convenings, held in partnership with other organizations, but also on its membership's attendance and participation in key international and regional forums, including the 2024 Summit of the Future discussions in the Caribbean Community (CARICOM) and the Economic Community of West African States (ECOWAS).

3.4. The application of existing international humanitarian law

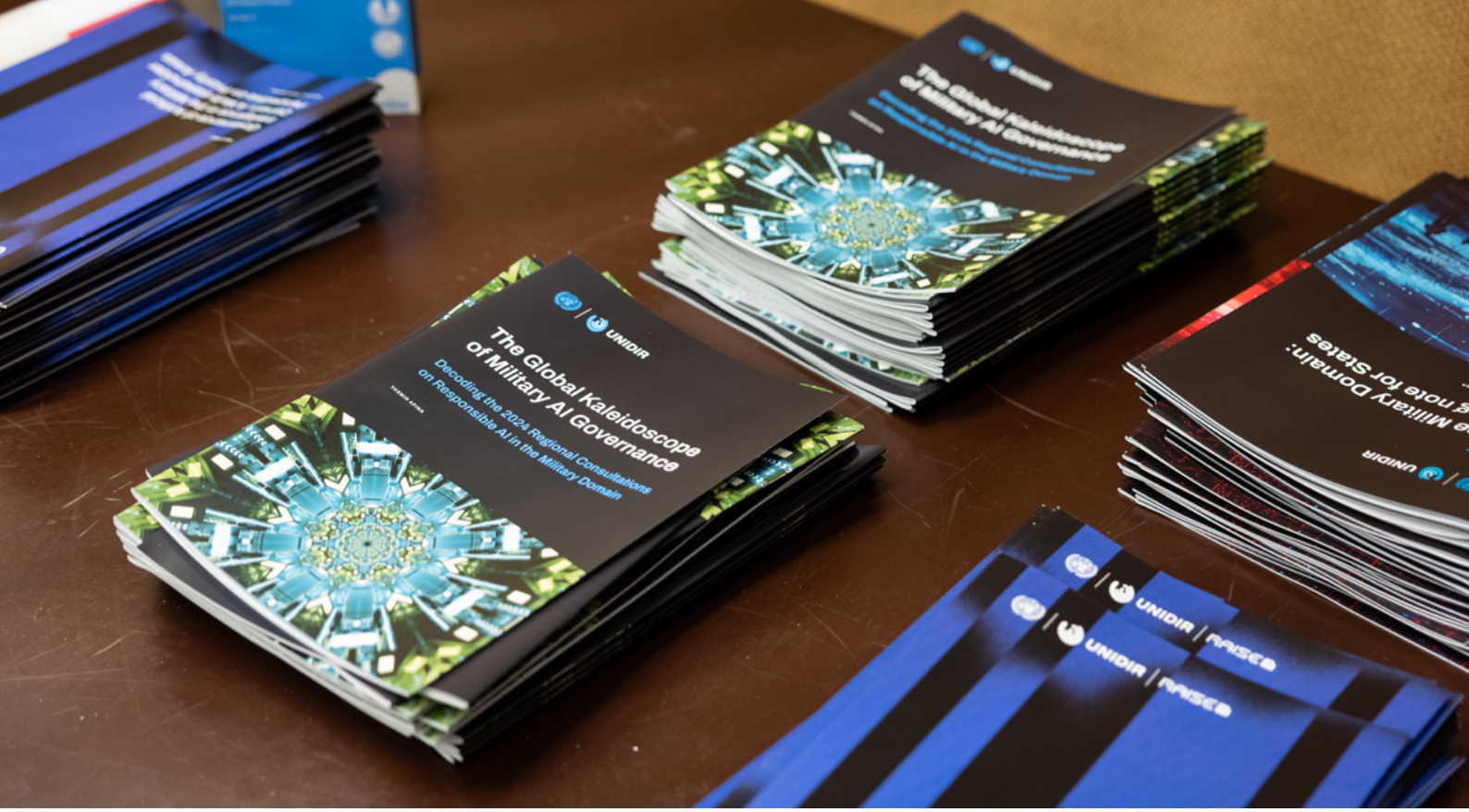
The development, deployment and use of AI in defence and security contexts do not happen in a vacuum: independently of the debate as to whether new regulatory frameworks are needed for military AI, IHL provides an existing set of rules and obligations applicable in armed conflict, including scenarios where AI technologies would be deployed and used. It is thus important for discussions surrounding the application of IHL to differentiate between *lex lata* (the law as it is) and *lex ferenda* (the law as it should be; e.g., the view that the law as it is remains insufficient and requires clarity amid the complexities that AI technologies bring to the application of IHL).[24]

With respect to AI and security, the human element is often presented as a *sine qua non* condition for legal compliance. Whether the human element is exercised through a certain degree of human supervision, oversight or control – and independently of the term and construct selected – this premise lies at the foundation of the views of many states and organizations. An alternative view is the argument that there is "no specific and precise obligation for [the] human element" in current treaty and customary IHL.[25] There is also the argument that, under some circumstances, the human element may constitute more of a liability, and violations of IHL remain the result of human acts and decisions. Independently of whether and how AI systems are used in defence and security contexts, legal responsibility will remain with states and individuals: they hold responsibility over the decision to procure, deploy and use AI systems, including through the conduct of the appropriate risk assessments, due diligence and other measures necessary for compliance. This leads to the view that, ultimately, discussion on the application of IHL is not necessarily about what the law says about and provides for the human element, but rather what the human element means for IHL compliance.

Initiatives are underway to elaborate views on the application of existing IHL in relation to AI in defence and security, and what the law requires across the life cycle of these technologies – from the pre-deployment stages to deployment and, eventually, the end of their life cycle. For example, the Asser Institute manages a project for a "Manual" on the international law applicable to AI in warfare. This academic initiative seeks to compile

24 For example, UNIDIR has conducted research to take stock of regional perspectives surrounding the application of IHL to LAWS. Albeit of different scope, a key finding of the consultations held as part of the project was that states were divided as to whether *lex lata* was sufficient, or further attention and focus were needed for *lex ferenda* (e.g., through the prohibition of all or certain types of LAWS). See Yasmin Afina, *Regional Perspectives on the Application of International Humanitarian Law to Lethal Autonomous Weapon Systems* (Geneva: UNIDIR, 2025), https://unidir.org/publication/regional-perspectives-on-the-application-of-international-humanitarian-law-to-lethal-autonomous-weapon-systems/.

25 As noted by Yasmin Afina (UNIDIR) in day 2's panel on the human element.



interpretations of existing international legal provisions governing the life cycle of AI-enabled systems, grounded in these technologies' technical characteristics and the realities of combat.[26] The Manual's scope covers IHL but also extends beyond, examining the application of *jus ad bellum*, international human rights law, international criminal law, and the nexuses of military AI technologies with space, the maritime domain and cyber.

3.5. The application of existing international human rights law

While international humanitarian law remains the most prominently cited body of law in defence and security contexts, international human rights law also applies to the development, deployment and use of these technologies. IHRL is more than a complementary framework to IHL; it is an independent and binding legal pillar for governing AI in security and defence that applies both in armed conflict (in conjunction with IHL) and in peacetime.

It was under the framework of IHRL that the issue of autonomy in security and defence contexts was initially brought up within the United Nations. The 2013 report on lethal autonomous robotics of the late Christof Heyns, who at the time was Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, is widely considered as the catalyst for these discussions within the organization.[27] Twelve years on, the report is still considered as being of relevance despite advances in both the technology and governance discussions. For instance, concerns around compliance with IHL and IHRL, the potential difficulty of translating context-dependent legal judgments into computer programmes, the risks of proliferation into the hands of non-state armed groups, and worries surrounding the removal of human deliberation from lethal decision-making all appear

26 The project was first publicly presented at AISE25 by Klaudia Klonowska (Asser Institute), Managing Director of the Manual project.

27 Human Rights Council, A/HRC/23/47.

in the report, echoing much of the concerns that persist today, including by the Secretary-General.[28]

IHRL provides a number of protections beyond the suite of obligations and other provisions set by IHL. Any absence of these protections can be argued to be an indicator of instability and violence.[29] This applies in the context of AI in defence and security, since a number of implications emerge during its development, deployment and use, including on the right to life, the right to liberty and security, the right to privacy, the right to non-discrimination, the right to remedy, as well as access to information.[30] States thus have three particular obligations to address these concerns: the duty to respect human rights; the duty to protect against abuses by third parties; and the duty to create an environment where human rights can be exercised, enjoyed and flourish. These obligations are marked against concerns that go beyond AI technologies: more broadly, mass data collection presents security risks that are even further emphasized through an ecosystem that incentivizes mass data collection, mass data storage and mass data sharing across borders. One example corresponds to the governance of data brokers and the processing of sensitive information about military personnel, which is recognized by many states as a national security problem.

As such, state obligations go hand in hand with those of businesses, particularly in recognition of the private sector's possible role in and influence over the operation of their digital products and services beyond their sale and eventual deployment. In this context, the United Nations Guiding Principles on Business and Human Rights (UNGPs)[31] offer a useful reference point to translate expectations, under international human rights law, for businesses. The B-Tech project of the Office of the United Nations High Commissioner for Human Rights (OHCHR) is specifically dedicated to the application of the UNGPs for technology companies.[32]

In the specific context of data, several recommendations and best practices can be established by both states and the private sector to support compliance with IHRL. These may include, but are not limited to:

The collection and processing of data must be legitimate

Proportionality-based limitations on the collection of data (i.e., not excessively collecting and using data beyond their intended purpose) could, for instance, serve as safeguards against risks of harm.

The conduct of impact assessments requires adequate resources

Data-protection authorities must, for instance, have adequate human and financial resources.

Systematic human rights due diligence assessments are needed

Beyond the identification, prevention and mitigation of human rights harms, particular attention is also needed to ensure remedies are accessible to victims of human rights violations and abuses.

---

28 As noted by Peggy Hicks (OHCHR) in day 1's opening panel, referring in particular to the Secretary-General's call for a legally binding instrument prohibiting LAWS that would operate without human control and that cannot comply with IHL.

29 As noted by Tim Engelhardt and Isabel Ebert (OHCHR) in a dedicated deep-dive on day 1: "'From Hero to Zero, or Zero to Hero?': Roles of State and Private Actors in Responsible Data Governance".

30 Engelhardt and Ebert.

31 OHCHR, "Guiding Principles on Business and Human Rights", 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

32 OHCHR, "B-Tech Project", https://www.ohchr.org/en/business-and-human-rights/b-tech-project.

The use of AI technologies in security and defence contexts may require specific measures

These could include, for instance, conflict-sensitive data policies, dedicated escalation procedures in case of data leakage or misuse, red-teaming exercises with respect to possible harms related to the collection, analysis and storage of data, and dedicated documentation processes for post-mortem assessments.[33]

4. Cross-cutting governance issues and challenges

4.1. Semantics

The elaboration of responsible AI frameworks in the military domain is complicated at the outset by a problem of language. Once common terminology becomes concrete, it creates a common basis for what is acceptable. The term "responsible AI" originates in the civilian sector – in industry and academia. Its meaning shifted as it was adopted by the defence community, with less emphasis on values such as societal well-being, privacy and explainability, and greater emphasis on reliability, safety and governability.

In the military domain, the reliability of a system bears directly on human lives and failure raises questions of legality, international law and the standards that armed forces are expected to uphold. The governance frameworks being shaped today are setting the parameters for how AI will be used in contexts where the costs of ambiguity are measured in human terms.[34] Even if the term "responsible" is understood as ensuring that technology consistently respects human rights and aligns with international law and established norms, its actual meaning in practice is harder to pin down. Some initial understanding comes from the long-standing corporate responsibility to respect human rights, as articulated in the United Nations Guiding Principles on Business and Human Rights, unanimously adopted by the Human Rights Council in 2011. Within the industry landscape, a degree of convergence is visible at the level of principle – frameworks across companies and initiatives have tended to cluster around fairness, reliability, security, privacy, safety and accountability – but shared terminology does not guarantee shared definitions.

Even within that adapted framing, foundational terms remain contested. Reliability in particular requires common definition and measurable thresholds, as systems need to meet a defined and operationalized benchmark for reliability in order to be deployed. These standards do not just apply to defence and security, but across industries.[35]

The problem is compounded by the changing nature and the stage of development of current AI systems themselves. As additional data and compute (i.e., computing power) are introduced, the emergence of new, unanticipated capabilities makes it genuinely difficult to anticipate failure modes or security and

33 For deeper insights on the application of IHRL in the context of AI in the military domain, see OHCHR, "Briefer on Human Rights and Artificial Intelligence in the Military Domain", 2025, https://www.ohchr.org/en/documents/brochures-and-leaflets/briefer-human-rights-and-artificial-intelligence-military-domain.

34 As noted by Arnault Valli (Head of Public Affairs at Comand AI) in the opening panel on day 2.

35 As noted by Michael Karimian (Microsoft) in the opening panel on day 2.

safety risks in advance. This uncertainty also appears in terminology.[36]

In the Track 2 dialogues between China and the United States on AI and international security, sustained confusion arose from the facts that a single term in Chinese covers both English terms "AI safety" and "AI security" and that "automatic" and "autonomous" carried divergent meanings across delegations. Shared terminology must therefore be treated as a governance prerequisite: a shared glossary, developed through genuinely interdisciplinary collaboration, is therefore a requirement for governance, rather than a secondary output.[37]

Without agreed definitions and measurable standards, normative convergence remains superficial. The gap between shared terminology and shared meaning is a substantive obstacle to the development of enforceable, interoperable governance frameworks

4.2. Trust and verification

Trust in the military AI context operates across multiple levels: between states diplomatically, between military actors operationally, and between public and private sector actors. It is characterized as a slow and fragile, but incremental process through sustained dialogue.[38]

At the interstate level, concrete mechanisms for trust-building include the sharing of risk-assessment methodologies, rigorous testing, evaluation, validation and verification (TEVV) processes, and the development of AI systems in realistic operational environments that allow failure modes to be identified before deployment.[39] AI systems should also be developed and tested in realistic operational environments, enabling the identification of failure modes before deployment. This stage also supports the development of interpretability tools that allow operators to appropriately calibrate their trust in system outputs. While the accumulated institutional wisdom of the arms control and disarmament community can be drawn upon, it must simultaneously be acknowledged that AI presents genuinely novel challenges that existing WMD-based frameworks may not fully address. Accordingly, differences must be confronted directly, rather than papered over with familiar analogies from arms control and disarmament.[40] TEVV processes are essential for establishing that systems perform reliably and predictably.[41]

The structural conditions for verification – the bedrock of arms control under the traditional "trust but verify" principle – are largely unfavourable in the AI context. AI development today is open by design, with meaningful barriers to entry being categorically different from the nuclear context. Moreover, unlike nuclear activity, which produces observable physical signatures detectable without the cooperation of the monitored party, AI capabilities leave no equivalent external trace: intelligent-seeming behaviour does not confirm AI use, and hardware capability does not prove deployment. Digital forensics represents the most direct verification method, but it presupposes a degree of openness that does not currently exist between major AI-developing states. Within the AI triad of data, algorithms and compute, hardware offers the most

36 As noted by David Sully (CEO at Advai) in the opening panel on day 2.

37 As noted by Xiao Qian (Tsinghua University) in the panel on "Knowledge and Capacity Building" on day 2.

38 As noted by Ambassador Robert in den Bosch (Disarmament Ambassador and Permanent Representative to the Conference on Disarmament, Netherlands) in the panel on "Trust-Building" on day 2.

39 In den Bosch.

40 Song.

41 In den Bosch.

tractable governance pathway: chips have serial numbers, are produced by a small number of manufacturers and are already subject to export control frameworks. However, verification cannot precede trust-building; it must follow it. The near-term priority is investment in confidence-building measures that progressively create the conditions under which more sophisticated verification becomes politically and technically feasible.[42]

4.3. Inclusivity

AI governance will face several inclusivity challenges along the North–South divide[43] and the growing AI digital divide[44] in terms of the distribution of technological capital, infrastructure and talent. Norm development for military AI must not be limited to technologically advanced countries: the United Nations is the only platform where inclusive, transparent and equitable discussions can take place. Developing countries without advanced AI capabilities must be at the table and must take part in creative mechanisms: open-ended working groups, independent scientific panels and technical expert groups already exist as models.[45] Regional representation, developmental diversity and the inclusion of states with significant military and technological capacity are all necessary conditions for legitimate and effective governance.[46]

Important concerns in the inclusivity debate in AI governance focusing on the Global South include gender representation, geographical and generational diversity and, crucially, military-technological inclusivity. Multilateral discussions resulting in frameworks negotiated without universal participation carry a structural vulnerability: states excluded from their development retain both the incentive and the standing to contest them, potentially reopening debates previously settled at the United Nations level. Genuine inclusivity in AI governance means including all states, regardless of the political differences it entails, as they yield the military and technological capacity to shape the real-world development and deployment of these systems.[47]

From the perspective of the African continent and the broader developing world, inclusivity carries a concrete and material meaning. With over 1.5 billion people and a substantial reservoir of emerging technical talent, Africa is not simply a stakeholder to be consulted, but a key region. It is therefore important that contributions are made to build up infrastructure (e.g., data centres and digital capacity) across the continent in order to ensure that this talent pool is cultivated and connected to the global AI ecosystem.[48]

---

42 As noted by Joon Baek (Columbia University) in the lightning talk on ”Lessons from the Nuclear Weapons Age for Managing AI Development” on day 2.

43 Judith Hanahan, “AI Divide: A New Fault Line We Cannot Ignore”, UNICEF, 29 January 2026, https://www.unicef.org/digitalimpact/blog/ai-divide-new-fault-line-we-cannot-ignore.

44 “World News in Brief: Tackling the AI Digital Divide, Deadly Migration Journeys, Lucy Hale Named New WFP Goodwill Ambassador”, UN News, 21 April 2026, https://news.un.org/en/story/2026/04/1167349.

45 Nakamitsu.

46 As noted by Ambassador Bial Ahmad (Permanent Representative to the United Nations, Pakistan) in the panel on ” Trust-Building” on day 2.

47 Kozyulin.

48 As noted by Moses B. Khanyile (Director, Defence Artificial Intelligence Research Unit (DAIRU), Faculty of Military Science, Stellenbosch University, South Africa) in the opening panel on day 2.

4.4. Pace of governance versus technological development

The pace of AI development presents a structural governance challenge. Speakers at AISE25 across the spectrum agreed that the speed of AI development is outpacing the ability of international governance to catch up effectively. Governance frameworks, legal standards and multilateral norms are challenged to keep pace with a technology that is already operational in military and security contexts, is already shaping decision-making processes, and is already testing the boundaries of existing international law. Innovation and research and development have been driven predominantly by speed and sophistication, rather than by responsibility or systematic attention to unintended consequences – a dynamic captured in the prevalent "Silicon Valley maxim" of moving fast and breaking things.[49] The consequences of that approach are now visible, and the case for reorienting even the early-stages of AI development around responsibility, reflection and a human-centric design has grown correspondingly stronger.[50] A slower, more deliberate pace of development is not inherently a constraint – it can create the space needed to anticipate harms and build solutions accordingly.

Technological development does not occur in a vacuum. It is shaped, catalysed and incentivized by political dynamics: the expansion of the defence technology industry in Europe, for instance, is a direct product of societies' perceived need for greater deterrence and protection. Private sector actors operate within those dynamics and are subject to market logic: profitability remains a governing consideration, which means that the values embedded in AI systems are partly a function of the incentive structures surrounding their development.

Industry actors broadly acknowledge that regulation will almost always trail behind technology, and that regulatory action in one jurisdiction will not prevent continued development elsewhere. The operative questions then become: Which values and legal standards are genuinely non-negotiable? And how can they be maintained even as the pace of development outstrips formal governance mechanisms.[51]

Even as AI transforms the conduct of warfare, the foundational questions remain of whether internationally agreed rules governing that conduct are respected and whether it represents, at minimum, a baseline that governance efforts must preserve.[52] The governance challenge is ensuring that, as these tools are adopted, the frameworks for information handling, data privacy and human oversight keep pace with the operational opportunities they create.[53]

---

49 As noted by Jibu Elias (Country Lead for India, Responsible Computing Challenge and Fellow, Mozilla) in the opening panel on day 2.

50 Elias.

51 Valli.

52 Valli.

53 As noted by Avishan Bodjnoud (United Nations Peace Operations – Chief Information Management Unit) in the deep-dive on "Leveraging AI to Support Knowledge Management for Uniformed Military Personnel in UN Peacekeeping Operations" on day 2.

5. Conclusion: Carrying the conversation forward from AISE25 to AISE26

AISE25 served as a useful waypoint to produce a grounded picture, as at March 2025, of the governance landscape surrounding the development, deployment and use of AI in security and defence. AISE26 convenes at a moment when several of the governance initiatives and processes identified at AISE25 have reached critical junctures, and when attention needs to move from principles to practice.

AISE26 will, in fact, meet after a dense period of institutional activities. Some of the key governance milestones that have been achieved between AISE25 and AISE26 include:

- The publication of the United Nations Secretary-General's report on AI in the military domain and its implications for international peace and security[54]
- The adoption by the United Nations General Assembly of resolution 80/58, a follow-up to resolution 79/239 on AI in the military domain and its implications for international peace and security,[55] which led to the organization of a three-day informal exchange on this issue to be held in Geneva on 15–17 June 2026[56]
- The organization of the third REAIM Summit, held in A Coruña, Spain, in February 2026
- The publication of the Strategic Guidance Report of the Global Commission on Responsible AI in the Military Domain[57]
- The launch of the UNIDIR-led project for the development of a Framework of Responsible Industry Behaviour for AI in the Military Domain, to be developed in partnership with the OHCHR and in consultation with industry representatives and governments[58]

Amid these advances in governance, several speakers at AISE25 pointed to the direction in which AISE26 and its subsequent editions need to focus their attention: as high-level principles on AI, security and ethics emerge hand in hand with the application of existing international law, specific guidance for their operationalization is now necessary. This guidance is required not only for members of the diplomatic community, policymakers, developers and technology providers, but also for the wider suite of actors involved in the ecosystem surrounding these technologies, from procurement officers to commanders and legal advisers.

As such, AISE26 is positioned to advance some of the governance questions for which AISE25 paved the way, including, among others:

- What role should the United Nations play to advance the governance of AI, security and ethics? What form should initiatives and processes within the United Nations take, and to what end?

---

54 General Assembly, A/80/78.

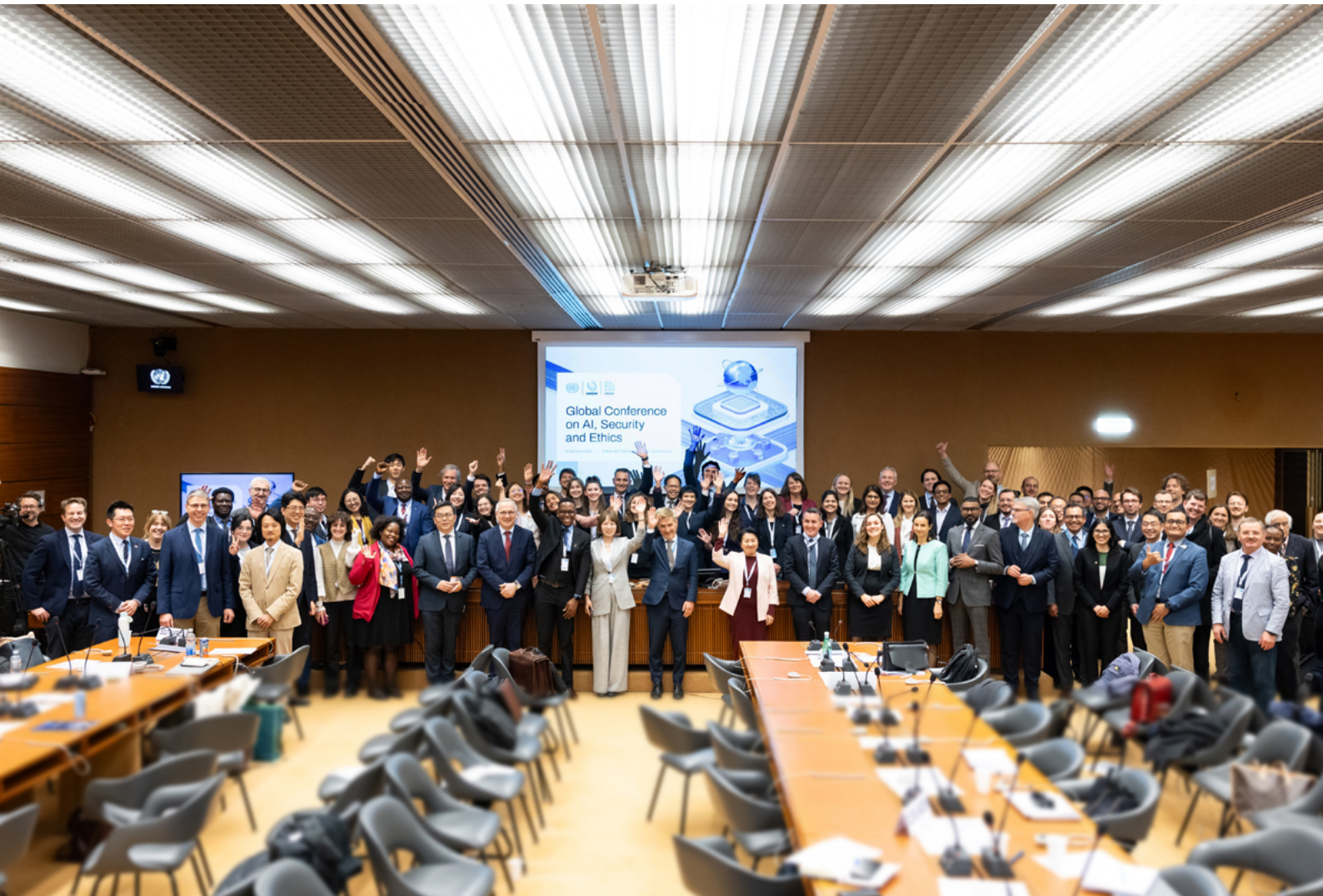
55 General Assembly, resolution 80/58.

56 Office for Disarmament Affairs, "UNODA Science, Technology and International Security Unit – Meeting", Meeting Place, 2026, https://meetings.unoda.org/unoda-stu-meeting/unoda-science-technology-and-international-security-unit-meeting-2026.

57 Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design*.

58 UNIDIR, "Framework of Responsible Industry Behaviour for AI in the Military Domain", 2026, https://unidir.org/framework-of-responsible-industry-behaviour-for-ai-in-the-military-domain/.

- Who should be at the table? What are some of the existing perspectives surrounding the role of the private sector, and what would constitute meaningful ways to provide the appropriate platform for structured engagement between states, industry and the wider multi-stakeholder community?
- What solutions could be considered and, eventually, implemented for the governance of AI, security and ethics – not only throughout its life cycle, but also across its multilayered stack? What best practices exist and which of them could either be replicated or serve as a source of inspiration?
- To what extent do regional differences and contexts add layers of sensitivity, and in what ways? What frameworks and initiatives would be most appropriate at the international, regional and national levels for the governance of these sensitive technologies?



Acknowledgments

Support from UNIDIR's core funders provides the foundation for all of the Institute's activities. This report was produced by UNIDIR's Security and Technology Programme, which is supported by the Governments of France, Germany, Italy, the Netherlands, the Republic of Korea and Switzerland, and Microsoft for its work on AI and autonomy. In addition, the Global Conference on AI, Security and Ethics 2025 was also supported by Advai.

UNIDIR extends its most sincere gratitude to all speakers, moderators, poster authors and audience members for their insightful presentations, comments and other contributions, which form the foundation of this report. UNIDIR also extends its profound gratitude to the members of the jury who helped review the abstracts received from UNIDIR's open call for proposals, which contributed to the conference's high calibre and the quality of the discussions: Dr. Alexi Drew, Major Jamal Mohamed Hassan, Calum Inverarity, Michael Karimian and Dr. Magdalena Pacholska. The evaluations were presented in the jury members' independent capacity and do not necessarily reflect the views or opinions of the jury members or of the organizations with which they work.

The authors wish to thank Dr. Giacomo Persi Paoli (UNIDIR) for advice, guidance, vision and support for the Global Conference and for his review of this report. Thanks for their support throughout the organization of the conference are also due to Jessica Lee Abowitz, Sapar Annayev, Asa Cusack, Jessica Espinosa Azcárraga, Anna Grangier, Edward Madziwa, Federico Mantellassi, Claudia Marquina and Mireia Mas Vivancos (UNIDIR), as well as to Elucidate Studios for the design support.

About UNIDIR

UNIDIR is a voluntarily funded, autonomous institute within the United Nations. As one of the few policy institutes worldwide that focus on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, it assists the international community in developing the practical, innovative ideas needed to address critical security problems.

About the UNIDIR Security and Technology Programme

Contemporary developments in science and technology present both new opportunities and challenges to international security and disarmament. UNIDIR's Security and Technology Programme aims to build knowledge and awareness about the international security implications and risks associated with specific technological innovations. It also convenes stakeholders to explore ideas and develop new approaches to address these issues.

Note

Citation

Yasmin Afina and Jan Hendrik Mannsperger, "AISE Markers Series – Benchmark I: Governance, Insights from the Global Conference on AI, Security and Ethics 2025", Geneva: UNIDIR, 2026.

About the authors

This report was produced by UNIDIR's Security and Technology Programme. It was drafted by Dr. Yasmin Afina and Jan Hendrik Mannsperger.

Photo credit

Cover photo generated with AI. Credit: Adobe Stock / Noy. All other photos featured were taken by Pierre Albouy at the Global Conference on AI, Security and Ethics 2025, 27–28 March 2025, Geneva. Credit: UNIDIR / Pierre Albouy.

Acronyms and abbreviations

AI	Artificial intelligence
AISE	Global Conference on AI, Security and Ethics
ASEAN	Association of Southeast Asian Nations
CCW	(Convention on) Certain Conventional Weapons
GC REAIM	Global Commission on Responsible AI in the Military Domain
GGE	Group of Governmental Experts
IHL	International humanitarian law
IHRL	International human rights law
IP	Intellectual property
IT	Information technology
LAWS	Lethal autonomous weapon systems
OHCHR	Office of the United Nations High Commissioner for Human Rights
RAISE	Roundtable for AI, Security and Ethics
REAIM	Responsible AI in the Military Domain
TEVV	Testing, evaluation, validation and verification
UAE	United Arab Emirates
UNGPs	United Nations Guiding Principles on Business and Human Rights
WMD	Weapons of mass destruction

UNIDIR

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

Palais des Nations
1211 Geneva, Switzerland

UNIDIR.ORG