REAIM SUMMIT 2027 | CONCEPT NOTE



RESPONSIBLE ARTIFICIAL INTELLIGENCE IN THE MILITARY DOMAIN · NAIROBI, KENYA

Strengthening Capability for Human Agency

Building Capability, Assurance and Responsibility for Peace and Security

THEME AND PILLARS

I Capacity and Capability

II AI-Enabled Decision-Making and Human Control

III Assurance, Safeguards and Responsibility

3	4	6	2
SUBSTANTIVE PILLARS	NAIROBI CALL ACTION AREAS	INDICATIVE DEEP DIVES	SUMMIT DAYS

DATES AND VENUE	PROPOSED OUTCOME	LEGACY PLATFORM
14–15 April 2027, Nairobi, Kenya	The Nairobi Call for Strengthening Capability for Human Agency	Moran AI & Cyber Centre of Excellence

01 Context and Nairobi Proposition

Artificial intelligence is moving from experimentation to operational use across the military domain. Applications now span intelligence and information analysis, command and control, logistics, surveillance, training and simulation, cyber operations, decision support, electronic warfare, and functions performed by uncrewed and increasingly autonomous systems.[1]

While these capabilities improve situational awareness, accelerate analysis and strengthen cyber defence, they also introduce critical operational and institutional dependencies. Systems can perform differently outside tested conditions, be manipulated by adversaries, compress decision time, rely on commercial infrastructure and suppliers, and make responsibility harder to trace across complex technology stacks.

The dual-use character of contemporary AI sharpens these questions. Many defence-relevant capabilities originate in civilian and commercial ecosystems before being adapted or integrated for military purposes, which places procurement, access to models and data, software updates, cloud and compute dependencies, supply-chain security and the movement of capabilities between civilian and military contexts at the centre of responsible use.[2]

The REAIM process has evolved alongside these developments. The Hague Summit in 2023 established a global platform for the responsible development, deployment and use of artificial intelligence in the military domain.[3] Seoul in 2024 advanced the Blueprint for Action around international law, human responsibility, appropriate human involvement, reliability and trustworthiness.[4] United Nations General Assembly resolutions 79/239 and 80/58 broadened the multilateral basis for this work and reinforced international cooperation, lifecycle responsibility and capacity-building.[5,6] A Coruña in 2026 moved the agenda towards implementation through practical work on responsible use, assurance and capacity.[7]

Nairobi should advance the REAIM process by focusing on the capabilities states, institutions and people need to exercise meaningful agency as AI systems become more capable and more deeply integrated into consequential decisions.

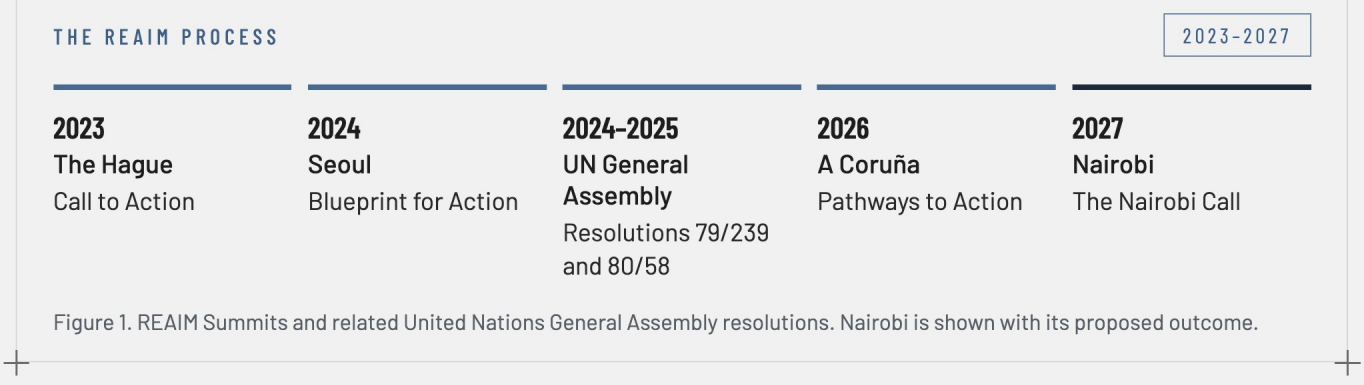


Figure 1. REAIM Summits and related United Nations General Assembly resolutions. Nairobi is shown with its proposed outcome.

1.1 Strengthening Capability for Human Agency

Human agency is the practical ability to understand a system, judge its capabilities and limits, determine the conditions for its use, question or reject its outputs, intervene when necessary, and remain responsible for the consequences of a decision. The concept extends established REAIM work on human responsibility and appropriate human involvement into contemporary questions of capability, assurance and safeguards.

Multimodal and agentic systems are expanding the range of tasks that can be delegated and the degree of authority systems can exercise across digital environments.[8] Current work on safeguards and assurance accordingly concentrates on evaluation, monitoring, limits on delegated authority, independent expertise and mechanisms for intervention, and in doing so clarifies the practical conditions for responsible action in the military domain.[9,10]

REAIM 2027 will examine those conditions through three substantive pillars, with industry and multi-stakeholder participation operating across all three as a working modality:

PILLAR I
Capacity and Capability

PILLAR II
AI-Enabled Decision-Making and Human Control

PILLAR III
Assurance, Safeguards and Responsibility

02 Purpose and Objectives

Under the theme "Strengthening Capability for Human Agency", REAIM 2027 will focus on the human, institutional and technological capabilities, operational practices and assurance arrangements required to translate responsible AI principles into practice. The Summit connects policy, military, legal and technical perspectives while recognising different national pathways for developing, procuring, evaluating and governing AI-enabled capabilities.

01 Strengthen the capabilities states and institutions need to develop, procure, evaluate and use AI applications responsibly in the military domain.

02 Examine AI-enabled decision-making and human control across advisory systems, delegated functions and varying degrees of autonomy, with human judgment, institutional responsibility and applicable international law central to operational practice.

03 Advance workable approaches to assurance, safeguards, testing, evaluation and international cooperation that support implementation beyond Nairobi.

03 Programme Architecture

The pillars form a connected progression: Pillar I enables human agency through capability; Pillar II examines how agency is exercised through decision-making and control; and Pillar III sustains agency through credible assurance, safeguards and accountability. The subtitles guide session development without restricting the scope of any pillar.

Each pillar examines the **current state of play**, the **challenges those developments now present**, and the **opportunities Nairobi can advance**.



Figure 2. Programme architecture.

3.1 Pillar I — Capacity and Capability

Enabling States and Institutions to Exercise Informed Agency

Meaningful agency depends on states and institutions being able to understand, assess and govern the systems they develop, procure or use, particularly where capability depends on commercial technologies, external infrastructure or systems developed elsewhere.

DIMENSION	STATE OF PLAY, CHALLENGES AND PROSPECTS
TRENDS	Military and security institutions now draw on a distributed AI ecosystem that spans defence establishments, commercial technology companies, cloud and compute providers, research institutions and specialised suppliers. States combine domestic development with procurement, partnerships and shared infrastructure, and technical decisions increasingly require expertise in models, data, cybersecurity, interoperability, system updates, integration and evaluation. The result is a wider spectrum of national capability. Some states develop advanced or specialised systems, while others primarily procure, adapt or integrate technologies developed elsewhere. Across these models, the ability to understand dependencies and evaluate performance has become central to responsible adoption.[11]
CHALLENGES	Responsibility can exceed institutional and technical capability. A state may remain accountable for a system while lacking the specialist expertise or independent evaluation capacity needed to verify supplier claims. Institutional capacity is also uneven. Technical expertise may exist without being adequately connected to doctrine, procurement, legal review, training, command arrangements or operational governance. Dual-use supply chains deepen these challenges by creating dependencies on commercial models, infrastructure, updates and components whose development and assurance processes may sit outside national defence institutions. These asymmetries can narrow the choices available to states and limit their ability to participate meaningfully in international rule-setting.
PROSPECTS FOR NAIROBI	Nairobi can move capacity-building from a general commitment to a practical implementation agenda by identifying the core institutional, technical and human capabilities that responsible adoption requires, including training, doctrine, procurement competence, legal review, testing and evaluation, cyber resilience, data governance, incident response and institutional oversight. The Summit can also advance models of shared and distributed capability, such as regional centres of excellence, shared evaluation facilities, professional military education, common training resources, access to independent expertise and structured international partnerships. These models widen national choice and agency while recognising that states participate in different parts of the technology stack.

3.2 Pillar II — AI-Enabled Decision-Making and Human Control

Advancing Human Judgment, Control and Responsibility Across AI Applications

AI-enabled decision-making extends beyond systems that assist human analysis. It includes systems that inform, recommend, execute delegated functions or operate with varying degrees of autonomy. The relevant questions concern the authority delegated, operational context, conditions for human judgment and intervention, and the responsibility attached to decisions and outcomes. This scope allows discussion of intelligence, cyber operations, electronic warfare, uncrewed systems and emerging applications without treating all AI as merely advisory.

DIMENSION	STATE OF PLAY, CHALLENGES AND PROSPECTS
TRENDS	AI applications are expanding across intelligence and information analysis, command and control, logistics, training, surveillance, cyber operations, electronic warfare, decision support and uncrewed systems. Uncrewed aerial, maritime and ground platforms increasingly combine AI-enabled sensing, navigation, coordination and mission adaptation, while AI is being applied to cyber defence, threat detection, vulnerability analysis and incident response. Agentic systems are increasing the number of tools, databases and operational systems with which AI can interact. Commercial and dual-use technologies are also reaching defence environments through procurement, adaptation and integration at a pace that can exceed traditional acquisition and review cycles.[12]
CHALLENGES	Performance established in controlled testing may not hold under new data, adversarial behaviour, degraded communications or operational pressure. Automation bias and compressed decision timelines can weaken critical judgement even where a person remains formally involved, and integration with sensors, communications systems, cyber tools, databases and uncrewed platforms makes system-level behaviour harder to anticipate. Cyber operations and electronic warfare introduce machine-speed interactions and active adversarial manipulation. Uncrewed and swarm systems raise questions of distributed autonomy, communications loss, mission adaptation and the conditions under which human intervention remains meaningful. And commercial and dual-use systems distribute responsibility across developers, suppliers, integrators, procuring authorities, commanders and operators.[13]
PROSPECTS FOR NAIROBI	Nairobi can make responsible use operational by organising part of the programme around applications and scenarios that test established principles in realistic conditions, including degraded and contested environments. Deep dives can examine how international law, doctrine, procurement, training and human-machine procedures operate across AI-enabled decision support, cyber operations, uncrewed and swarm systems, electronic warfare, intelligence, surveillance and reconnaissance, logistics and information environments. The Summit can identify where AI appropriately supports human judgement, where stronger safeguards or limitations are required, and how institutions should respond when systems operate outside expected parameters. These deep dives can generate practical guidance for doctrine, procurement, training and governance.

3.3 Pillar III — Assurance, Safeguards and Responsibility

Building Confidence Through Evaluation, Oversight and Accountability

Assurance provides the evidence required to decide whether a system can be relied upon for a particular purpose and context. Safeguards translate that evidence into practical boundaries, controls and mechanisms for intervention. Responsibility remains with the people and institutions authorised to make consequential decisions.

DIMENSION	STATE OF PLAY, CHALLENGES AND PROSPECTS
TRENDS	Testing and evaluation, verification and validation, red-teaming, cybersecurity assessment, monitoring, incident reporting and independent review are now established components of AI assurance. Assurance is also shifting from pre-deployment assessment to a lifecycle discipline, because systems change through software updates, retraining, new data, integration and interaction with external environments. Safeguards practice is moving towards stronger evaluation, monitoring and controls as systems gain capability or authority. Cybersecurity has become integral to assurance, covering resilience to adversarial manipulation, data poisoning, model compromise, unauthorised access and supply-chain vulnerabilities.[14]
CHALLENGES	Military assurance operates under severe structural constraints: systems are frequently proprietary or classified, operational environments diverge sharply from test beds, and access to underlying models and training data is routinely restricted. States with limited technical capacity may therefore depend on supplier assurances they cannot readily reproduce or challenge. Technical safeguards have limited effect when disconnected from procurement rules, doctrine, legal obligations, command arrangements and operational procedures. Responsibility also becomes harder to trace as more actors participate across the lifecycle, from model and infrastructure providers to integrators, commanders and operators.
PROSPECTS FOR NAIROBI	Nairobi can advance an integrated approach to assurance that connects technical evidence with operational, legal and institutional decisions. Priority areas include testing and evaluation, red-teaming, cyber resilience, monitoring, incident reporting, access controls, independent assessment, human-machine protocols and mechanisms for intervention when systems move beyond defined parameters. The Summit can examine what information states should require from suppliers, how assurance should be built into procurement and update cycles, how independent evaluation capacity can be made more widely accessible, and how incident learning and confidence-building measures can support responsible practice. Norms of responsible state behaviour in cyberspace offer transferable lessons here, including incident reporting, points of contact, emergency-response mechanisms, critical-infrastructure protection and capacity-building.[15]

04 Cross-Cutting Priorities

Four considerations cut across the three pillars.

International law, human responsibility and human agency

Legal review, command responsibility, accountability and appropriate human judgement should be embedded throughout the programme, together with attention to the practical conditions that allow individuals and institutions to exercise meaningful agency as system capabilities increase.

Dual-use, procurement and supply-chain resilience

Commercial models, infrastructure, data services and components move between civilian and military contexts, so procurement, vendor relationships, software updates, export controls, assurance and proliferation risks bear on all three pillars.

Cybersecurity, data and information integrity

The programme should address AI used in cyber operations, the security and resilience of AI-enabled systems, and the data provenance, access, classification, quality and integrity on which system performance depends.

Inclusion, capacity and human-security perspectives

Regional perspectives and uneven technical capacity should shape the programme and the Nairobi Call, with attention to shared capability, access to expertise, Women, Peace and Security, humanitarian considerations and civilian protection.[16]

05 Multistakeholder Participation

Industry, academia, civil society, technical communities and international organisations will participate across the programme because expertise, infrastructure and responsibility are distributed across the AI ecosystem.

Governments and defence institutions retain distinct responsibilities for national security, international law, command and the use of force. Industry develops and operates significant parts of the models, infrastructure and applications on which states may depend. Academia and technical communities contribute research, testing and independent expertise, while civil society and humanitarian actors contribute perspectives on accountability, protection and wider societal consequences.

The programme will therefore combine expert exchange, scenario exercises, demonstrations, military leadership dialogues and practitioner roundtables on Day One, with ministerial and Chiefs of Defence Staff engagement on Day Two. Multistakeholder participation will be embedded across the three pillars and the Summit's working formats.

DAY ONE · 14 APRIL

Expert exchange, scenario exercises, demonstrations, military leadership dialogues and practitioner roundtables

DAY TWO · 15 APRIL

Ministerial and Chiefs of Defence Staff engagement

06 Indicative Deep Dives

A limited number of focused deep dives will test the Summit's propositions against concrete applications and operational conditions:

01 **AI-enabled decision support and meaningful human judgement**	02 **Cyber operations and the cybersecurity and resilience of AI-enabled systems**
03 **Uncrewed aerial, maritime and ground systems, including swarming and ISR**	04 **Dual-use technology, responsible procurement and supply-chain assurance**
05 **Assurance across the lifecycle, including testing, evaluation, verification, validation and incident learning**	06 **Strategic stability, escalation and decision speed in command-and-control environments**

Training, doctrine, professional military education, data governance, information integrity and relevant humanitarian considerations will be integrated across these discussions.

07 Proposed Summit Outcome: The Nairobi Call

REAIM 2027 will propose an action-oriented outcome:

PROPOSED OUTCOME DOCUMENT

The Nairobi Call for Strengthening Capability for Human Agency

An Action Framework for Capability, Assurance and Responsibility in the Military Domain

The Nairobi Call will build on previous REAIM outcomes and relevant United Nations resolutions by translating areas of convergence into a practical implementation framework. Modelled on previous action-oriented frameworks, it will set out non-binding, voluntary and direction-setting actions that states and participating stakeholders can pursue within their respective sovereign and institutional mandates, organised around four action areas:

ACTION AREA I	ACTION AREA II	ACTION AREA III	ACTION AREA IV
Build Capability for Responsible Action	**Advance AI-Enabled Decision-Making and Human Control**	**Strengthen Assurance, Safeguards and Accountability**	**Deepen International Cooperation and Implementation**

Figure 3. The four action areas of the proposed Nairobi Call.

The Nairobi Call will be open to voluntary endorsement by states and participating stakeholders that support its objectives. Endorsers may also make voluntary public pledges identifying specific actions they intend to advance. Endorsement will not require a pledge, so each endorser can support the Action Framework while determining its own implementation pathway and timeline.

Industry, academia, civil society, technical communities and international organisations may make aligned commitments within their respective mandates, while the responsibilities of states and military authorities for national security, the use of force and compliance with international law remain distinct.

08 Expected Outcomes

REAIM 2027 will seek to establish a practical implementation agenda that continues beyond Nairobi. The principal outcomes will be:

OUTCOME	DESCRIPTION
1. The Nairobi Call	Translates areas of convergence on human agency, capability, responsible use, assurance and responsibility into a practical Action Framework.
2. Voluntary commitments and partnerships	Allow states and participating stakeholders to advance specific elements of the Nairobi Call within their respective mandates.
3. Follow-up mechanism	Connects implementation of the Nairobi Call to subsequent REAIM Summits, relevant United Nations processes, regional cooperation and technical networks.

09 Nairobi Legacy: Institutionalising Capability

The Summit should connect its capacity-building agenda to sustained institutional cooperation. As a host-country contribution, Kenya proposes the **Moran AI & Cyber Centre of Excellence** as one platform for advancing the Nairobi agenda beyond the Summit, including through its proposed contribution to the NEXUS knowledge-institute network.

The Moran Centre can support training, professional military education, research, testing and evaluation, cyber resilience and international knowledge partnerships beyond April 2027. Its role would be to translate elements of the Nairobi agenda into practical capability for Kenya, the region and participating partners, working with international centres of excellence, research institutions and technical networks.

10 Nairobi's Contribution to the REAIM Process

Nairobi can advance the next stage of the REAIM process by strengthening capability for human agency. States and institutions need the ability to understand systems, evaluate evidence about performance, determine the conditions governing deployment and delegated authority, exercise judgment and intervene when necessary, and remain accountable for consequential decisions. Capability enables agency; decision-making and human control put it into practice; assurance and safeguards sustain it throughout the lifecycle.

REAIM 2027 can therefore move the process from agreement on responsible principles towards the capabilities, practices and institutional arrangements required to implement them.

Endnotes

1 UNIDIR, *Artificial Intelligence in the Military Domain and Its Implications for International Peace and Security: An Evidence-Based Road Map for Future Policy Action* (Geneva: United Nations Institute for Disarmament Research, 2025).

2 UNIDIR, *Governance of Artificial Intelligence in the Military Domain: A Multi-Stakeholder Perspective on Priority Areas* (Geneva: UNIDIR, 2024); see also UNIDIR, *Evidence-Based Road Map* (2025).

3 Government of the Netherlands, *REAIM 2023 Call to Action*, Summit on Responsible Artificial Intelligence in the Military Domain, The Hague, 2023.

4 Republic of Korea, *REAIM Summit 2024 Blueprint for Action*, Seoul, 2024.

5 United Nations General Assembly, Resolution 79/239, *Artificial intelligence in the military domain and its implications for international peace and security*, 2024.

6 United Nations General Assembly, Resolution 80/58, *Artificial intelligence in the military domain and its implications for international peace and security*, 2025.

7 REAIM 2026, *A Coruña Pathways to Action* and Summit materials, A Coruña, 2026.

8 World Economic Forum, *Making Agentic AI Work for Government: A Readiness Framework* (Geneva: WEF, 2026).

9 World Economic Forum, *AI Agents in Action: A Playbook for Trusted Adoption, Authorization and Scaling* (Geneva: WEF, 2026).

10 Minderoo Foundation, work on AI safeguards, accountability and national-security considerations, 2026.

11 UNIDIR, *The Global Prism of Military AI Governance: Reflections from the 2025 Regional Consultations on Responsible AI in the Military Domain* (Geneva: UNIDIR, 2026).

12 UNIDIR, *Evidence-Based Road Map* (2025).

13 UNIDIR, *Governance of Artificial Intelligence in the Military Domain* (2024).

14 Minderoo Foundation (2026); World Economic Forum, *Making Agentic AI Work for Government* (2026).

15 UNIDIR, *From Cyberspace to AI: Translating Norms of Responsible State Behaviour in Cyberspace to AI in the Military Domain* (Geneva: UNIDIR, 2026).

16 UNIDIR, *The Global Prism of Military AI Governance* (2026).