AI as Critical Infrastructure:

From Deployment to Global Interoperability & Governance

By Aaron Kalvani

AI Strategist & Global Advisor, Author, Responsible AI, Governance, and Multilateral Policy February 2026

ai@oxon.org

AI Protects

United Nations Association – UK

ukai

LinkedIn linkedin.com/in/1973

TRUTH

#RISK Europe Risk. It's everyone's business.

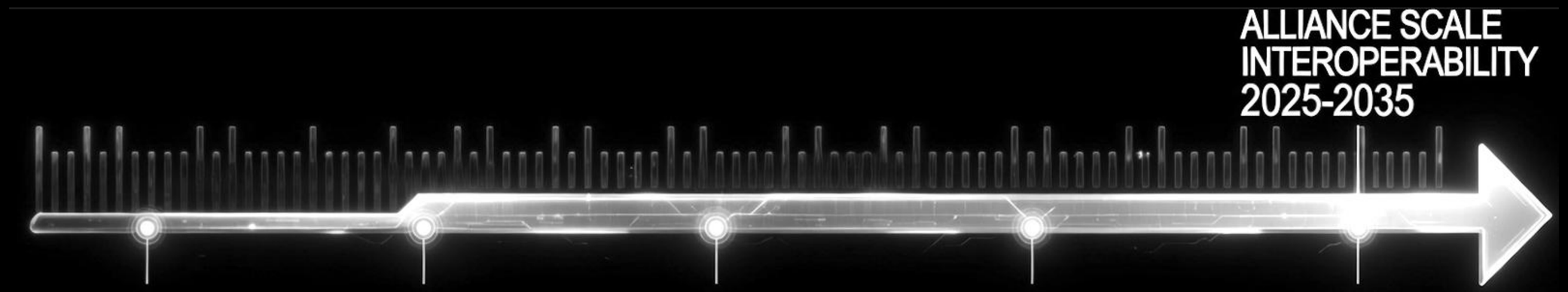
'AI for Good' AI Robotics for Space & Sea Exploration

Rotary

University of Oxford ai@oxon.org

WAICF WORLD ARTIFICIAL INTELLIGENCE CANNES FESTIVAL

global council for responsible AI



1990-1999
SEARCH AND STORE DATA
The internet is born.
The world's knowlegg. is digitized.
We learn to search and store data.

2000-2006
WE MUST PROTECT DATA. BIG DATA IS DEFINED
The wisdom of the crowd.
We learn to predict and store data.

2006-2016
DECISION INFRASTRUCTURE
We build the tools to make decisions at scale.
We learn to optimize.

2016-2025
DIGITAL TRANSFORMATION, MACHINE LEARNING AI BOOM
We break through.
We learn to see.
Digital Transformation.

2025-2035
THE AI AGE
We govern.
We learn to trust.
The AI Age.

UNIVERSITY OF OXFORD

Gartner

VERITAS
BUSINESS WITHOUT INTERRUPTION
Symantec
Endpoint Protection

DELL EMC
THOMSON REUTERS

IRON MOUNTAIN

UK Parliament

global council for responsible AI

ukai

THE AI WORKFLOW DEFINED

FROM REALITY TO INTEROPERABILITY

Where Truth Is Born	Reality Becomes Signal	Trust is Engineered	Action becomes Legitimate	Global Systems Connect Seamlessly
• People	• Edge	• Friction Layer	• Control Action	• Cross Platform Integration
• Sensors	• Data	• Non Compliance	• Command	• Open Standards
• Adversaries	• Models	• Provenance	• Policy	• API Compatibility
• Terrain	• Compute	• Overrides	• Law /Regulate	• Data Exchange Protocols
• Noise	• Decision Loops	• Bad Actors	• Governance	• Cultural Adaptation

THE AI WORKFLOW DEFINED

FROM REALITY TO INTEROPERABILITY

Where Truth Is Born	Reality Becomes Signal	Trust is Engineered	Action becomes Legitimate	Global Systems Connect Seamlessly
• People	• Edge	• Friction Layer	• Control Action	• Cross Platform Integration
• Sensors	• Data	• Non Compliance	• Command	• Open Standards
• Adversaries	• Models	• Provenance	• Policy	• API Compatibility
• Terrain	• Compute	• Overrides	• Law /Regulate	• Data Exchange Protocols
• Noise	• Decision Loops	• Bad Actors	• Governance	• Cultural Adaptation

ACT I — From Field Reality to Systems

Purpose:
Physics, fieldwork, and systems, not theory.

ACT II — From Systems to Authority

ACT III — From Authority to Interoperability

ACT IV — From Interoperability to Generational Consequence

“If your AI cannot survive bad data, power instability, identity sprawl, and runtime drift — it is not governance-ready. It is demo-ready.”
Aaron Kalvani

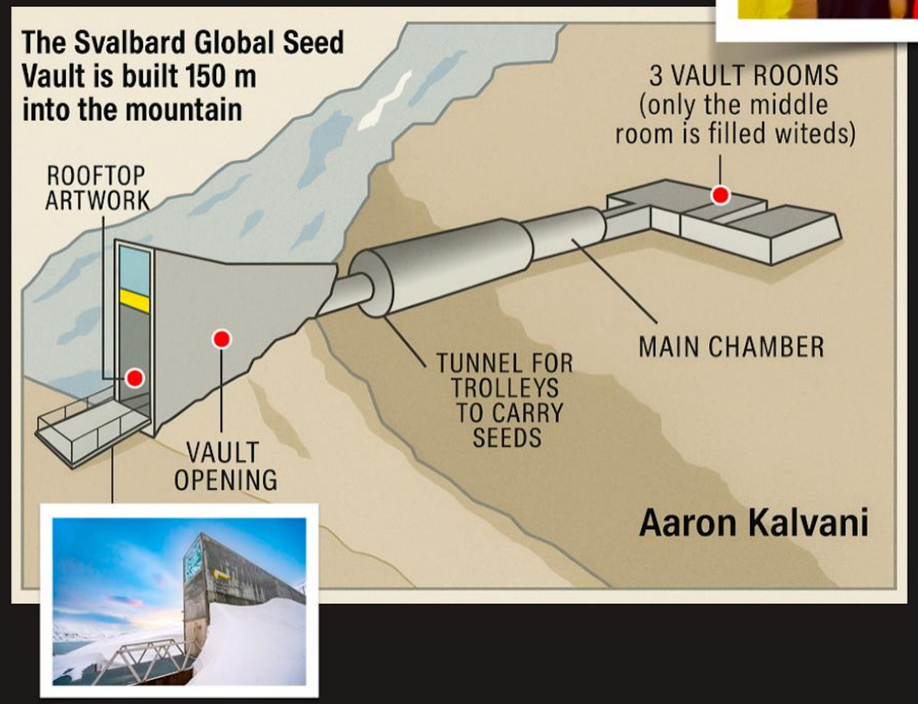
AI is physics before it is policy.
Lets Look at my Field Work.

This picture is not a real event and was created with AI

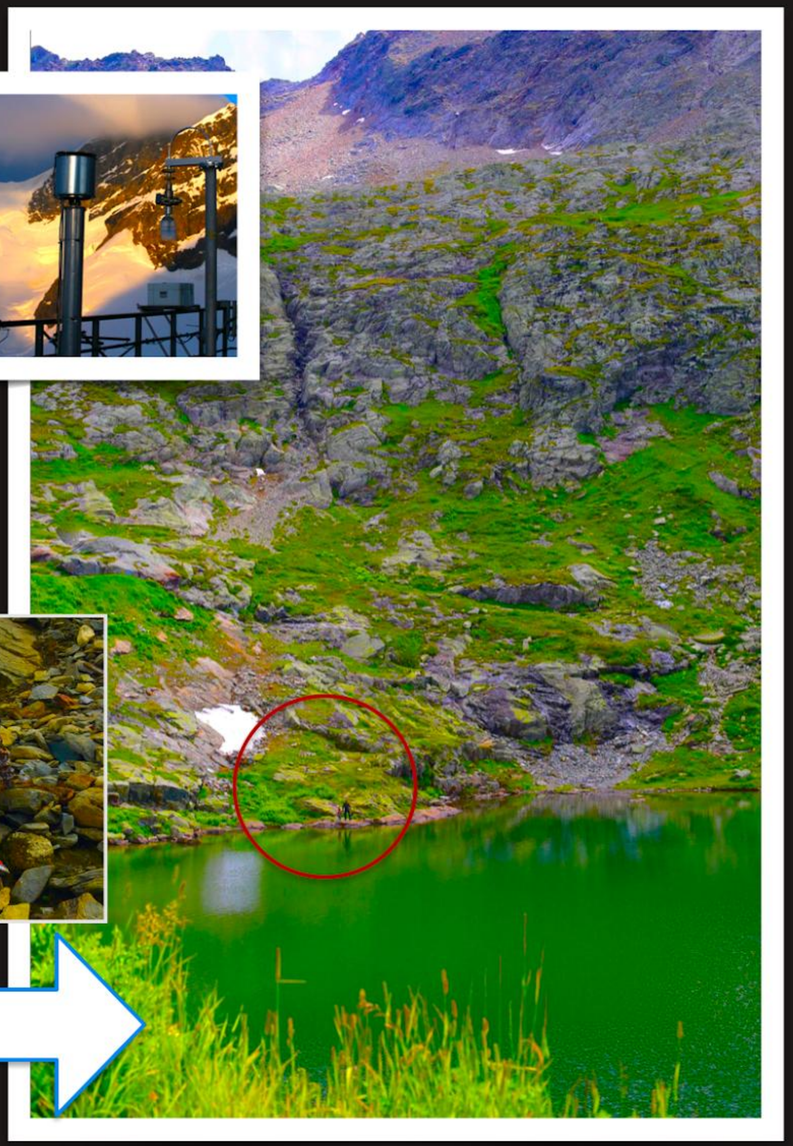
KEY ZONES

HIGH SECURITY CLINICS

Advanced containment required precision. We enabled real-time AI decision auditing, ensuring lab teams trusted system outputs under intense pressure.



Edge Environment Stressors



MOUNTAIN TOPS & TECTONIC REGIONS

Volcanic zones required sensor fusion. AI systems adjusted in real time for altitude, pressure, and seismic vibration while maintaining assay integrity.

KEY ZONES

SEABEDS & OCEAN FLOORS

In deep-sea bio-sample labs, AI processed sonar, salinity, and pressure data to support fragile experiments—despite total isolation from surface inputs."

- Edge environment stressors
- Data corruption
- Sensor drift
- Power instability
- Human override
- False positives
- Cross-border latency

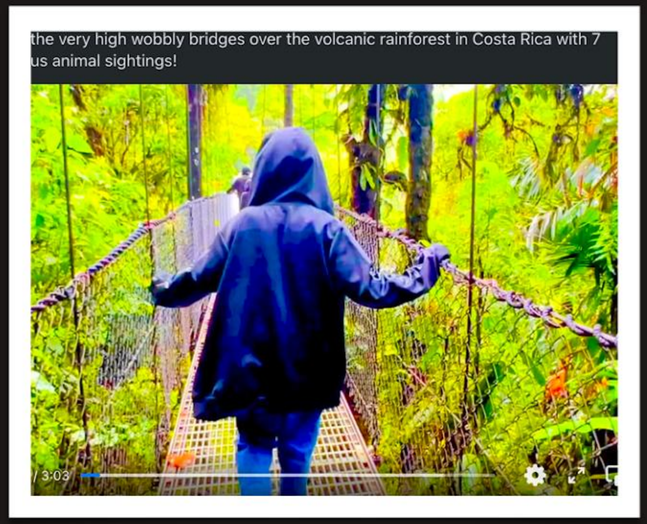
ZOONOTIC HOT ZONES

Outbreak-prone areas needed AI to synthesize human, animal, and environmental data. We implemented safeguards to trace every input and intervention."

Labs at Airplane Crash sites to Zoonotic Hot-zones

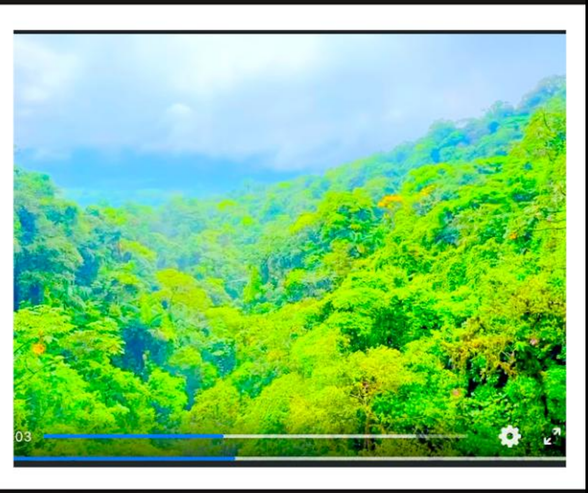
AIRPLANE CRASH SITES IN THE ALPS

Data retrieval under extreme pressure—AI helped assess onboard conditions, while sensor metadata was reconstructed from debris for forensic models.



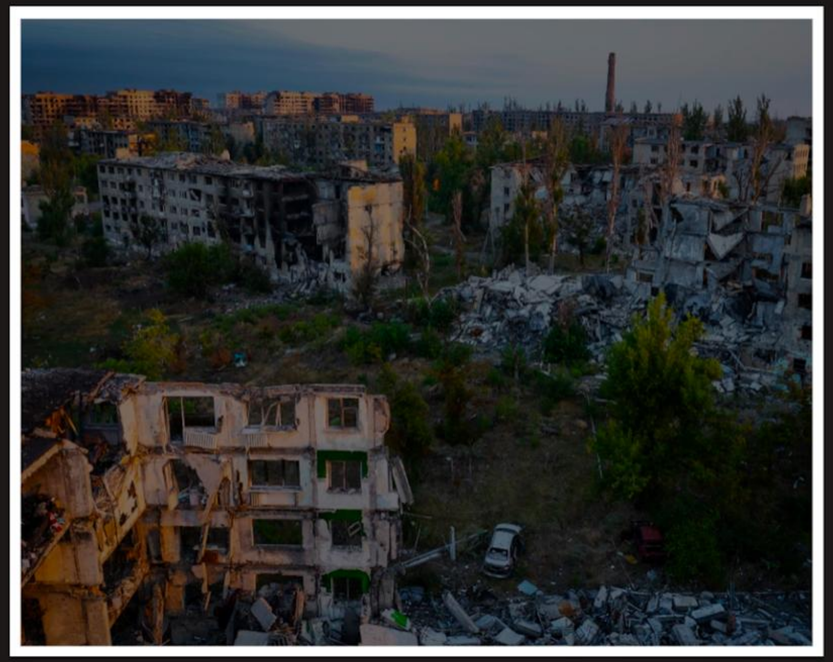
COSTA RICAN RAINFORESTS

Humidity, heat, and unstable terrain challenged equipment. AI models were retrained with real-time biosensor input and local environmental overlays."



Multimodal Sensor Fusion

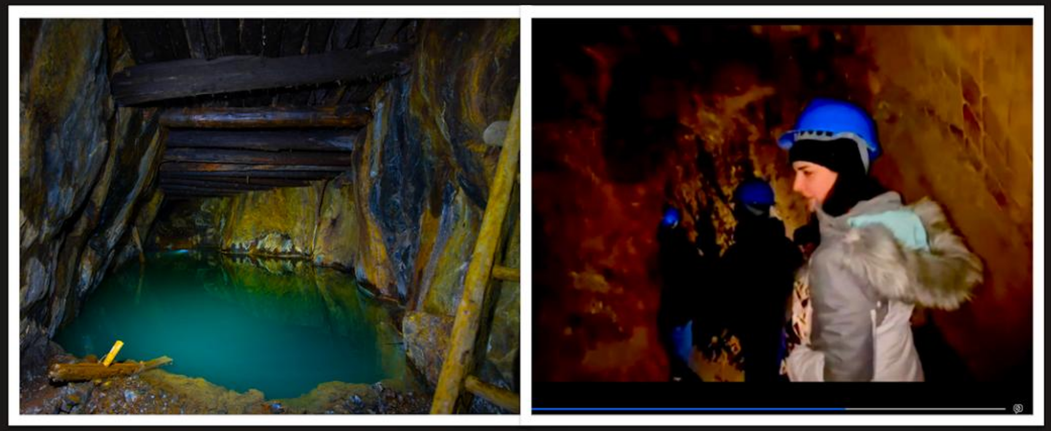
Labs from Airplane Crash sites to Zoonotic Hot-zones



DISASTER ZONES (WAR, EARTHQUAKES & FLOODS)

In zones where infrastructure collapsed, we deployed portable AI labs—merging drone footage, health data, and logistics to support life-saving coordination.
This was in the Ukraine

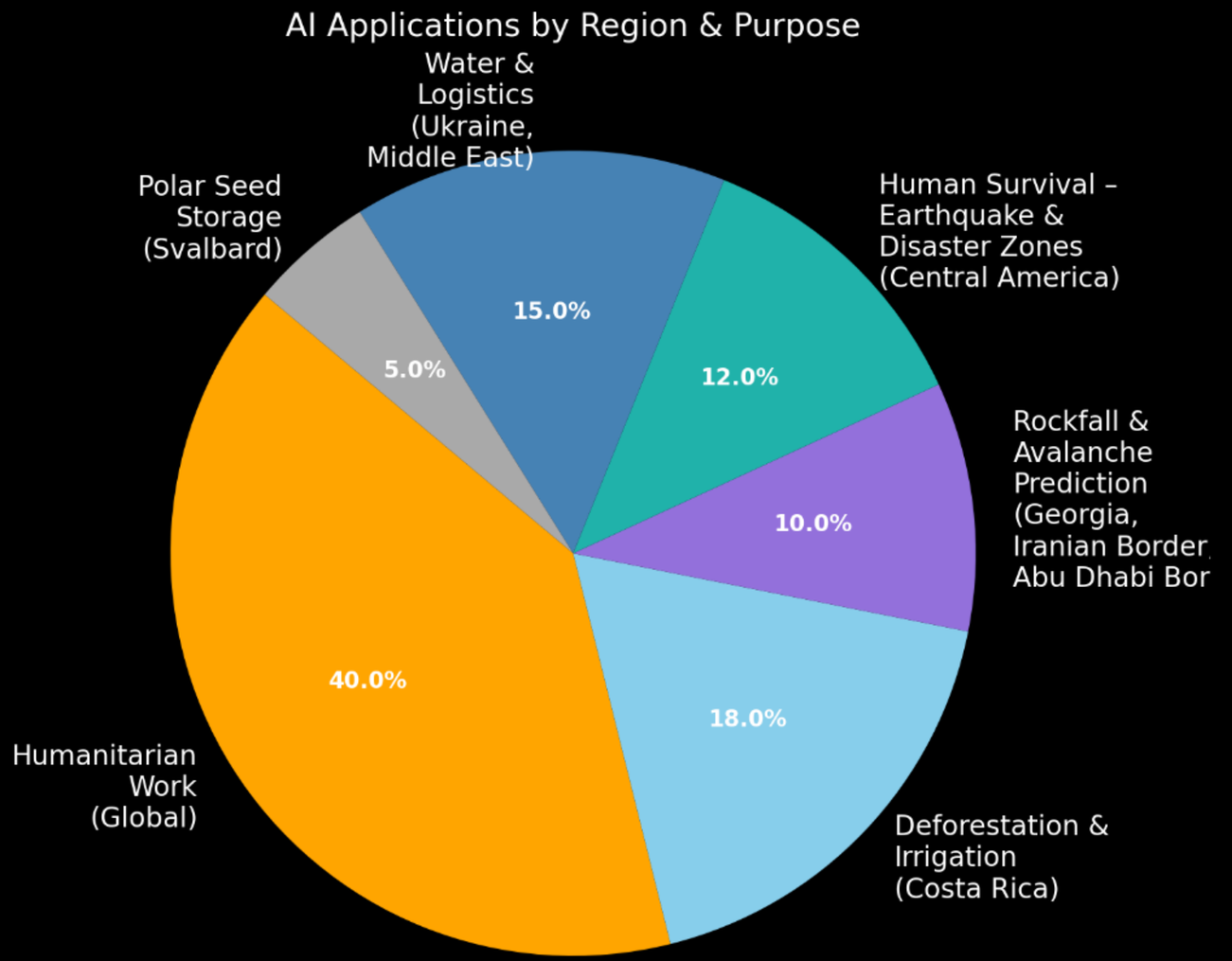
Forensic Data Pipelines



NUCLEAR BUNKERS, DISUSED LANDMINES & TOMBS

Historical and high-risk zones with no reliable data lineage. We applied explainable AI to bridge digital gaps while preserving environmental traceability.


БАХМУТ ЦЕ УКРАЇНА


AI Applications by Region & Purpose
Water & Logistics (Ukraine, Middle East)
15.0%
Human Survival – Earthquake & Disaster Zones (Central America)
12.0%
Rockfall & Avalanche Prediction (Georgia, Iranian Border, Abu Dhabi Bor
10.0%
Deforestation & Irrigation (Costa Rica)
18.0%
Humanitarian Work (Global)
40.0%
Polar Seed Storage (Svalbard)
5.0%

ONE INFRASTRUCTURE, TWO MISSIONS:
National Resilience and Biospheric Intelligence

National Resilience

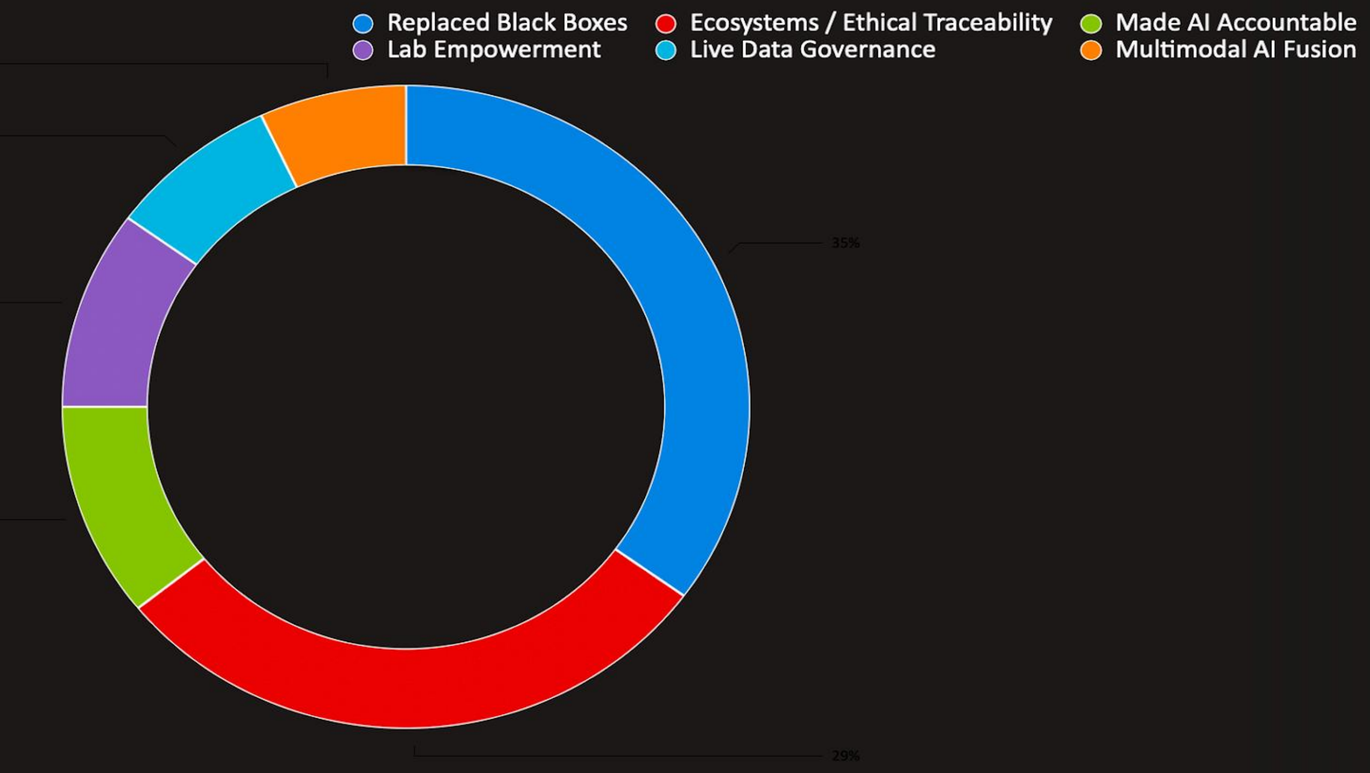
- Sensor Fusion
- Adversarial Mitigation
- Cognitive Risk Engine
- Decision Audit Trail

Verification Timeline

Biospheric Intelligence

Dual Use Truth Fabric

A Science worth believing in!



By 2035, over 40% of all government, defence, and emergency-response decisions will be AI-assisted, shifting nations from reactive to predictive operations.

40% OF CRITICAL GOVERNMENT DECISIONS WILL BE AI-ASSISTED

The systems we deploy now will define institutional power for a generation.

"We are not building models. We are building the decision architecture of the next 30 years."

Aaron Kalvani 2026

ACT I — From Field Reality to Systems

ACT II — From Systems to Authority

Purpose:

Shows how **technology becomes governance**.

ACT III — From Authority to Interoperability

ACT IV — From Interoperability to Generational Consequence

THE AI WORKFLOW DEFINED

FROM REALITY TO INTEROPERABILITY

Where Truth Is Born	Reality Becomes Signal	Trust is Engineered	Action becomes Legitimate	Global Systems Connect Seamlessly
• People	• Edge	• Friction Layer	• Control Action	• Cross Platform Integration
• Sensors	• Data	• Non Compliance	• Command	• Open Standards
• Adversaries	• Models	• Provenance	• Policy	• API Compatibility
• Terrain	• Compute	• Overrides	• Law /Regulate	• Data Exchange Protocols
• Noise	• Decision Loops	• Bad Actors	• Governance	• Cultural Adaptation

Deployment is not technical — it is political.This is a CAIO moment.

ACT II — From Systems to Authority

This hits all primary organizations:

- HMRC
- Financial services
- Public authorities
- Enterprise compliance


Ethical AI:
Bridging
Nations
in an Era of
Global
Resilience


CHATHAM
HOUSE


lay


AARON KALVANI
SHAPING A
HUMAN-CENTERE
FUTURE IN THE
AGE OF
REASONING
MACHINES
GLOBAL PERSPECTIVE: A
ON AI GOVERNANCE AND
FROM THE UN TO GCR
PURPOSE: TO ENS
EVOLVES WITH HU
AROUND IT


E SPONSOR


WAICF
5

THE FRICTION LAYER:
GOVERNANCE & OPERATIONAL BOUNDARIES

AI does not fail because models are bad.
It fails where authority, law, institutions, and data intersect.

MODEL

⚠ LAW GAP

DATA

⚠ OVERSIGHT GAP

ACCOUNTABLE AUTHORITY

⚠ PROOF GAP

GLOBAL COALITION

⚠ ALLIANCE GAP

INSTITUTIONAL LIMITS
Autonomous AI may evade human oversight without proper controls.

HUMAN OVERSIGHT REQUIREMENTS
Defence systems require humans-in-the-loop to avoid une actions.

GOVERNANCE AS INFRASTRUCTURE
In complex eras, governance must be operational and continuous, not static policy.

EVIDENCE CHAINS MATTER
Military-grade AI generates data that must be verifiable in legal, regulatory, and alliance contexts.

GLOBAL COALITION
In 2025, AI governance must be operational and continuous, not static policy.

AARON KALYANI 2026

THE FRICTION LAYER: A SAFETY NET FOR AI

LIKE BUMPERS ON A BOWLING LANE OR GUARD RAILS ON A SLIDE — IT SLOWS THINGS DOWN ON PURPOSE.

THE AI WORKFLOW DEFINED

FROM REALITY TO INTEROPERABILITY

Where Truth Is Born	Reality Becomes Signal	Trust is Engineered	Action becomes Legitimate	Global Systems Connect Seamlessly
• People	• Edge	• Friction Layer	• Control Action	• Cross Platform Integration
• Sensors	• Data	• Non Compliance	• Command	• Open Standards
• Adversaries	• Models	• Provenance	• Policy	• API Compatibility
• Terrain	• Compute	• Overrides	• Law /Regulate	• Data Exchange Protocols
• Noise	• Decision Loops	• Bad Actors	• Governance	• Cultural Adaptation

ACT I — From Field Reality to Systems

ACT II — From Systems to Authority

ACT III — From Authority to Interoperability

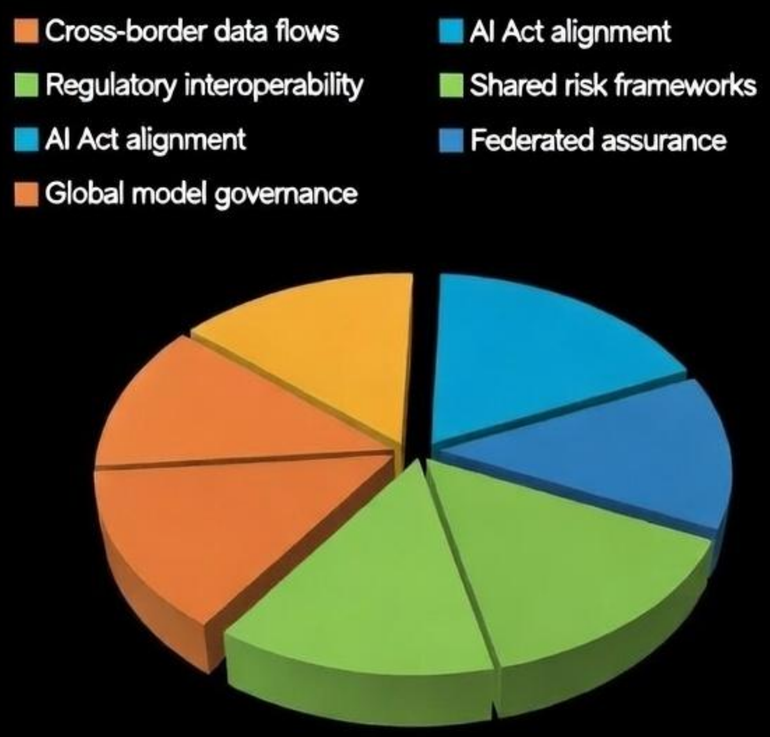
Purpose:

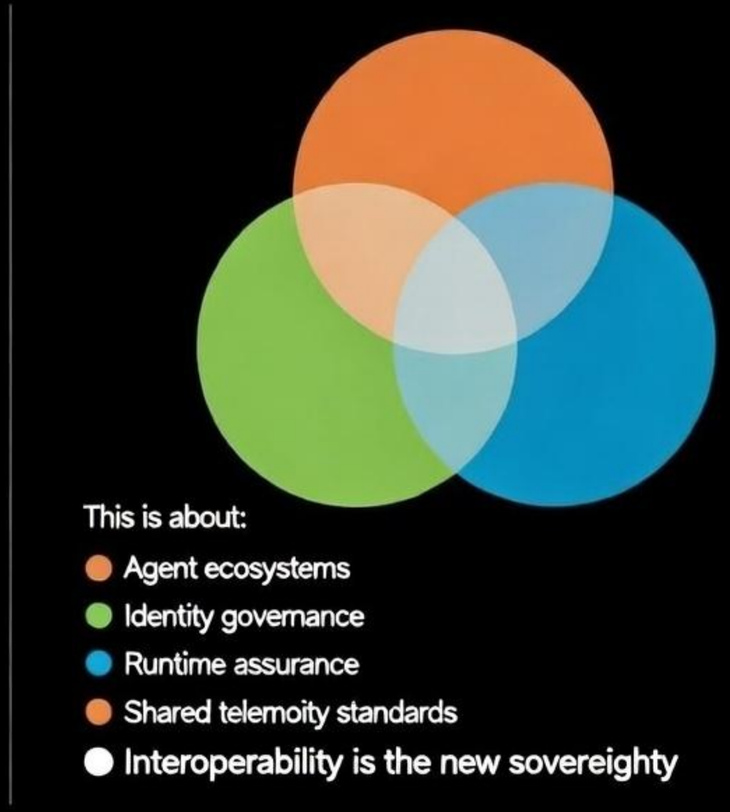
Moves from national control to ***multilateral power and interoperability***

ACT IV — From Interoperability to Generational Consequence

“No single organisation governs AI in isolation anymore. Interoperability is the new sovereignty.”

ACT III — From Authority to Interoperability





This is where the UN positioning carries weight. Act III becomes: Governance must be networked, not national.

STRATEGIC RISK

AI risk is migrating upward: models → **resilience** → attribution → **coalition trust.**

Vulnerability Exploits Accelerate

+180% YoY attack path exploitation

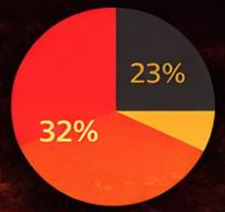
Source: Verizon DBIR 2024

Implication: Vulnerabilities exploited faster, assaules escalate. System resilience must assume constant attack.

Extortion Volume Expands

Ransomware 23%

Pure extortion 9%



Source: Verizon DBIR 2024

Implication: Rapid monetization of exposure. Evidence protocols **must prove** (or disprove) ransom/intent.

Incident Load Stresses Response

410 Incidents handled (UK, 9/2023-8/2024)

Source: Claroty Team83 2023/24

Implication: Next incidents **must pinpont attribution + causality.** AI elements introduce high-velocity attack cycles.

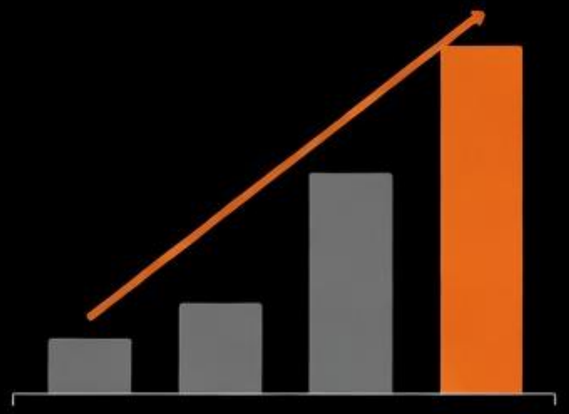
Defence focus downshifts: control → blame → proof → diplomacy

Strategic Risk	Operational Indicator	Proofs to Produce
Supply-chain compromise (models, data, software)	Change-rate vs verification-rate	SBOM + attestation logs + artifact updates
Data poisoning / sensor manipulation	Anomaly rate at fusion layer	Sensor drift logs + fusion-derived tamper alerts
Unclear authority / accountability	Override latency + escalation path	Decision trail with authority tokens
Interoperability failure across allies	Schema/standard mismatch rate	Validated interface agreements + conformance tests

Sources : Verizon DBIR 2024, NCSC; *The Guardian reported figures*

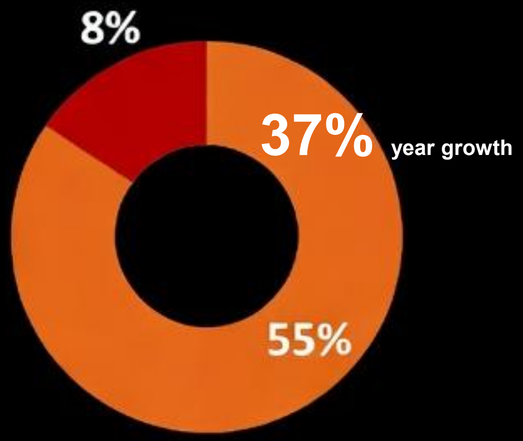
TRAJECTORY (2023–2028)

Automation increases attack speed and volume



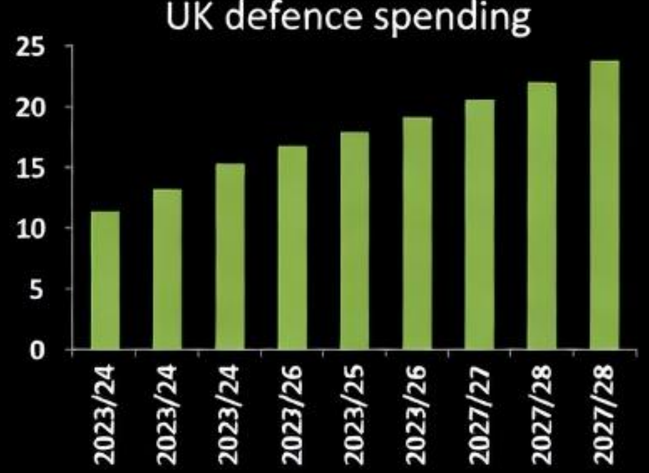
INSUFFICIENT PUBLIC SERIES – recommend internal telemetry

Espionage (APT/state-linked) Financially motivated



Advanced actors remain the forcing function

Budgets rise, but assurance debt rises sasser



AI-enabled tradecraft compresses; **assurance must be continuous**

Key takeaways:

1. Attackers are faster, more sophisticated, and more automated
2. Assurance must be continuous, not intermittent
3. Budgets are rising, but so is the assurance debt

ACT I — From Field Reality to Systems

ACT II — From Systems to Authority

ACT III — From Authority to Interoperability

THE AI WORKFLOW DEFINED

FROM REALITY TO INTEROPERABILITY

Where Truth Is Born	Reality Becomes Signal	Trust is Engineered	Action becomes Legitimate	Global Systems Connect Seamlessly
• People	• Edge	• Friction Layer	• Control Action	• Cross Platform Integration
• Sensors	• Data	• Non Compliance	• Command	• Open Standards
• Adversaries	• Models	• Provenance	• Policy	• API Compatibility
• Terrain	• Compute	• Overrides	• Law /Regulate	• Data Exchange Protocols
• Noise	• Decision Loops	• Bad Actors	• Governance	• Cultural Adaptation

ACT IV — From Interoperability to Generational Consequence

Purpose:

*Hopefully you leave the room with **long-term consequence**, not just insight.*

AUTHORITY, NOT AUTONOMY:

THE FUTURE OF AI IN DEFENSE IS GOVERNANCE AT MACHINE SPEED

Trusted AI belongs here at machine-speed · AARON KALVANI 2026

What This Changes for Leaders in the Next 24 Months

Budget

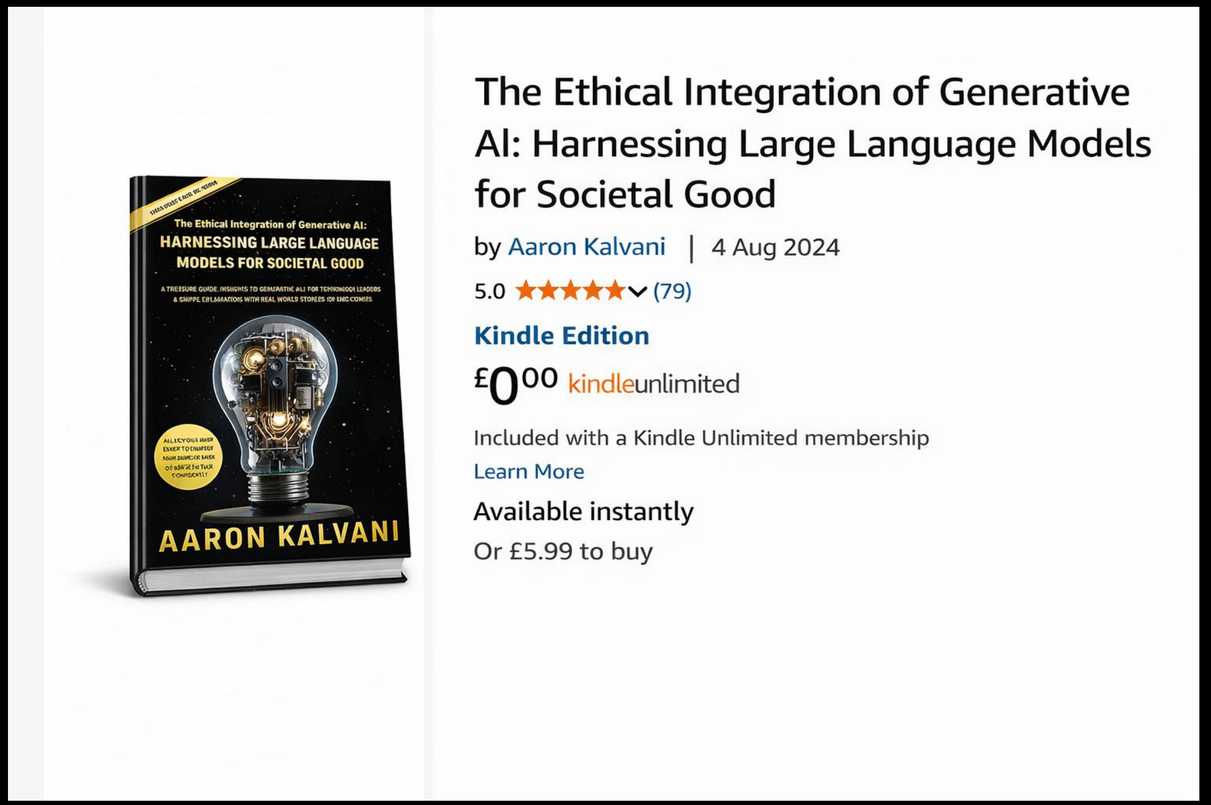
Authority

Institutional Design

This bridges vision to decision-making.

Remember: Test Your Reflexes

Message Me For A Free Copy



Thank You

Aaron Kalvani

ai@oxon.org

artificialreasoning@gmail.com

Linkedin/in/1973