KLUZ PRIZE℠
FOR PEACETECH

The Annual Frontier Report 2026

Benchmarking report on frontier technologies serving peace and humanity.

Published by the Kluz Prize for PeaceTech. September 2026.

Every generation of technology arrives with a promise of peace and a capacity for harm. This one is no different — except that the choice between the two is being made right now, and mostly by default.

About this report

The Annual Frontier Report 2026 is the inaugural edition of the Kluz Prize for PeaceTech's benchmark report on frontier technologies serving peace and humanity. Our mission is to establish the global benchmark for PeaceTech. Each year we seek to identify the most important trends, the pioneering use cases, and the breakthrough innovations shaping the future of peace, human dignity, and human flourishing — and to track how they evolve from breakthrough ideas to real-world impact.

It is intended as an essential reference for those who will determine whether frontier technology serves peace or is turned against it: **technology entrepreneurs, builders, engineers and programmers, investors and venture capitalists, philanthropists, and the global media.**

This inaugural 2026 edition draws on almost five years of the Kluz Prize for PeaceTech, including more than **500 applications from innovators in over 82 countries**, together with extensive desk research, the Prize's ongoing scan of the field, and Kluz Ventures' investment experience. The report is organized around **nine frontier trends**, each illustrated through real-world use cases drawn from the Prize's global applications, track record, research, and practical experience, together with a catalogue of more than 100 PeaceTech initiatives spanning the entire conflict cycle. The full index appears at the end.

The report also draws on **Kluz Ventures'** (https://www.kluzventures.com/) investment experience across frontier technologies. Kluz Ventures' long-term supercycle investment strategy — spanning public markets, private markets, and fund-of-funds — provides an additional perspective on the identification and assessment of emerging technological trends. Additionally, Kluz Ventures' strategy claims to take into account the growing international conversation on the ethical governance of frontier technologies, which holds that technological progress should always serve the human person, uphold human dignity, promote the common good, strengthen solidarity, and advance authentic human flourishing.

What This Report Is Not

This report is deliberately **not an exhaustive review of PeaceTech**. It does not seek to provide a comprehensive account of the field's history, evidence base, or lessons learned—positive and negative—nor does it attempt to evaluate every technology or intervention associated with peacebuilding. Important work already exists documenting both the promise and the limitations of technology in conflict and peace settings, including the risks of unintended consequences, exclusion, surveillance, manipulation, and harm.

Nor is this report intended as a **practitioner's guide for humanitarian or peacebuilding organizations** seeking to deploy technology responsibly in particular contexts. Such deployment requires deep contextual knowledge, conflict sensitivity, community engagement, safeguarding, and careful attention to the "do no harm" principle. A frontier report cannot substitute for those practices or for the more detailed guidance developed by organizations working directly in these environments.

Finally, this is **not a research agenda for scholars and scientists**. Many important questions about the effectiveness, ethics, governance, and long-term societal consequences of PeaceTech remain unresolved, and a substantial research community is better positioned to identify and investigate them. We point to the reader for selected resources in the accompanying reading list for these purposes.

About the Kluz Prize for PeaceTech

The Kluz Prize for PeaceTech is an annual global initiative dedicated to celebrating, recognizing, and accelerating the innovative use of emerging technologies in service of peace and humanity — to save lives, prevent conflict, foster peace, and safeguard human dignity and universal human rights. It is an initiative of **Kluz Ventures**. Winners and distinguished participants since 2022 include Magnolia Foundation, Commit Global, Aerobotics7, and Common Space, alongside VIEWS, Project Didi, the Human Rights Data Analysis Group, Lunasonde, the Humanitarian OpenStreetMap Team, UNOPS, and Anadyr Horizon — many featured in this report.

More information: www.kluzprize.org · info@kluzprize.org

Thank you to Francesco Bosco and Jamon Van Den Hoek for taking the time to review earlier versions of this report.

Contents

1. Introduction: PeaceTech

Conflict has become the background condition of international life, and technology now sits at its center. Drones, autonomous systems, artificial intelligence, AI-enabled targeting, satellites data, space technologies, data infrastructure, quantum technologies, nuclear technologies, and the deliberate spread of inaccurate information and manipulated data have become defining features of modern conflict. Vast sums flow into technologies of war; comparatively little flows in the opposite direction — technologies designed from the outset to save lives, protect human dignity, prevent violence, and rebuild trust. **That is PeaceTech. And this report is its annual benchmark.**

PeaceTech is the field of science, engineering, and technology dedicated to serving humanity: protecting dignity, saving lives, reducing suffering, strengthening resilient societies, and building the infrastructure that supports human flourishing. It spans the whole conflict cycle — preventing conflict, protecting civilians during it, supporting humanitarian response, accelerating recovery and reconciliation, and strengthening the long-term foundations of peaceful societies.

PeaceTech is distinct from both war and defense technology. *War technology* is designed to project force and conduct offensive operations. *Defense technology* is designed to detect, deter, defend against, and neutralize threats. Meanwhile *PeaceTech* is designed to save lives, protect human dignity, prevent conflict, reduce suffering, and rebuild the conditions for lasting peace. The distinction lies not in the technology itself, but in its purpose, governance, and intended outcomes. And the field is best defined by its clearest cases: demining robotics, conflict early warning, and evidence collection for accountability are unambiguous; the harder edges are judged on the merits, not admitted or refused by label — that innovation should strengthen human dignity, expand human agency, protect the vulnerable, and contribute to the common good rather than becoming an end in itself.

This report makes one central argument: the frontier has moved and continues to accelerate. The tools that defined PeaceTech even a few years ago — threat dashboards, mediation platforms, fact-checking services, SMS reporting, satellite snapshots — remain essential, but they are no longer the frontier. The action, the risk, and the opportunity have shifted to nine emerging trends. The bulk of this report documents them, one by one, through the innovations already putting them to work.

2. Methodology

This report identifies the frontier technologies most likely to shape peace and humanity over the coming decade. Rather than cataloguing every innovation, it benchmarks technologies by their potential contribution to saving lives, preventing conflict, protecting civilians, strengthening resilient societies, and rebuilding peace.

The 2026 edition draws on almost five years of the Kluz Prize for PeaceTech, more than 500 applications from innovators across the world, independent desk research, and ongoing engagement with technology builders, entrepreneurs, engineers, programmers, researchers, humanitarian organizations, investors, venture capitalists, governments, and international institutions.

Each use case has been assessed against six criteria, classified by maturity (Established, Emerging, or Frontier), then clustered around common themes, and organized within one of the report's nine frontier trends:

- **Peace relevance:** the credibility and directness of the use case's contribution to peace, human dignity, and human flourishing.
- **Technical maturity:** how proven the underlying technology is, from research to deployment.
- **Operational readiness:** whether the technology performs reliably in real-world settings, integrates into operational workflows, and can be sustained in practice.
- **Governance and legitimacy:** the strength of oversight, accountability, ethical safeguards, and institutional arrangements governing the technology's use.
- **Dual-use / offense-defense assessment:** the likelihood that the capability could be repurposed for harmful or offensive uses, and whether those risks can be effectively mitigated.
- **Scalability:** the potential of the use case to achieve the scale required to address the problem effectively.

Throughout the report, use cases are classified as **Established**, **Emerging**, or **Frontier**, and each trend receives an independent assessment of **Risk (1–5)** and **Opportunity (1–5)** — the two axes that converge in the matrix at the end of the report. The use cases are supported by examples, some of which being dual use.

How to read this report

Section 3 documents the **nine frontier trends** that structure this year's report, each with a snapshot, a risk-and-opportunity score, a funding verdict, and illustrative use cases tagged **Established**, **Emerging**, or **Frontier**. Section 4 sets out how to judge any application. Section 5 makes the investment case. Section 6 brings them together in the risk–opportunity matrix. The full 100-use-case index closes the report. In Section 7 we outline trends for a decade ahead and conclude with an index of PeaceTech use cases in Section 8.

3. The nine frontier trends

Nine shifts define the PeaceTech frontier in 2026. Each moves the field from a capability that is now mature toward one that is emerging or barely begun — and each is where investment, talent, and governance attention should now concentrate. For every trend we give the signal, where it stands, its risk and opportunity, a funding verdict, and the use cases already demonstrating it.

It is important to note that conflict-affected communities are key stakeholders in each of the below trends. Their lived expertise is critical in ensuring these technologies are implemented responsibly for the given context.

Trend 1 — From analytic AI to agentic AI

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
AI that acts, not just predicts	Emerging; first real deployments	Mediators, UN, foundations, conflict-affected communities
RISK ● ● ● ● ○ *acts rather than predicts, so error and manipulated data carry real consequences, can be corrected by strong governance*	**OPPORTUNITY** ● ● ● ● ○ *high leverage on the acting bottleneck; mediation and dialogue are underfunded*	

The first generation of AI for peace classified and predicted: it identified language associated with incitement and escalating violence, assessed conflict risk and analyzed satellite imagery. The frontier generation *acts*. Agentic systems run simulations, generate negotiation options, and facilitate dialogue between parties — moving PeaceTech from describing a situation to intervening in it. That shift multiplies both the leverage and the stakes of every design choice, because an agent that proposes a course of action carries responsibility a classifier never did. As the capabilities of agentic AI become more advanced each day, the importance of human judgement in the implementation of AI for peace has never been more critical.

The trend is visible across the conflict cycle, from anticipating a crisis to modelling its resolution:

- **Agentic AI geopolitical simulation** [Emerging] — models how decision-makers behave under pressure, simulating the misperception and escalation dynamics that drive crises · *Anadyr Horizon decision-maker modelling — Kluz Prize 2025 distinction (Use of AI for Peace)*
- **AI peace-scenario modelling** [Emerging] — used generative techniques and retrieval-augmented generation to model war-termination scenarios for Ukraine · *CSIS Futures Lab Ukraine scenarios (RAG)*
- **AI conflict-ripeness analysis for negotiations** [Emerging] — applies NLP and large language models to read when a conflict is ripe for resolution · *Project Didi (Israel/Palestine media analysis) — Kluz Prize 2023 distinction (Innovative Use of AI/ML)*
- **Agentic AI multi-party dialogue facilitation** [Frontier] — agentic facilitation of multi-party dialogue: credible, and not yet deployed at scale · *No large-scale deployment yet*
- **Empathy-building agentic AI between opposing groups** [Emerging] — empathy-building agentic AI between opposing groups, still at the pilot and research stage · *Stanford Peace Innovation Lab;*

Investment Strategy. Fund with strong human oversight and audit requirements. *(risk 4/5 · opportunity 4/5)*

Trend 2 — From single machines to autonomous and swarm robotics

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
Coordinated fleets, not lone units	Established → frontier at scale	Demining agencies, defense-adjacent funders, conflict-affected communities
RISK ●●●●○ *the autonomy that enables scale is directly dual-use*	**OPPORTUNITY** ●●●●○ *the only credible path to clearing contamination at the scale the problem demands*	

A single demining drone is now an established tool. The frontier is coordination: swarms and autonomous fleets that could clear contaminated land at a scale manual methods cannot approach. The stakes are concrete — Ukraine alone has on the order of 139,000 square kilometres of estimated contamination (2025), over twice the estimated land contaminated in Vietnam over the last 50 years, which no crew-by-crew effort can clear in any acceptable horizon. The same autonomy that makes this possible is what makes the category dual-use, and lethal autonomous weapons systems should not be allowed. This is why this trend needs the moral test more than most.

- **Drone-based demining** [Established] — autonomous ground robotics for demining and UXO clearance · *Aerobotics7 EAGLE A7 (Ukraine) — Kluz Prize 2024 winner, HALO Trust Ukraine R&D; Draganfly/Autonome Labs demining mesh; IOS/CMAC DMR robot*
- **Swarm drones for large-scale demining** [Frontier] — the scale-up bet, still under development and extension of single-drone systems · *HALO Trust AI-drone mapping (Ukraine);*
- **Underwater autonomous vehicles for marine demining** [Frontier] — where peace applications trail military ones · *GICHD-tracked marine ROV trials;*
- **Drone delivery of medical supplies** [Established] — drones delivering medical supplies to frontlines, showing the logistics backbone this trend builds on · *Draganfly (Ukraine frontlines, 35 lb payload)*

Investment Strategy. Back demining-specific applications; do not invest in weaponisation dual uses and lethal autonomous weapons systems. *(risk 4/5 · opportunity 4/5)*

Trend 3 — From satellite data to space infrastructure and services

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
From observing Earth to enabling peace from space	Emerging; commercial space infrastructure maturing fast	Space & commercial space companies, investors, governments, space agencies, humanitarians, conflict affected communities
RISK ●●○○○ *mostly benign; the main risk is dependence on private operators who can switch it off*	**OPPORTUNITY** ●●●●● *a continuous watch, democratizable to local actors, and maturing fast*	

The first generation of PeaceTech relied on satellite imagery to understand what had already happened. The next generation is built on **space infrastructure and services** that continuously support life on Earth. Low-earth-orbit constellations, resilient satellite communications, navigation systems, synthetic-aperture radar, orbital computing, and advanced space sensors are turning space into critical infrastructure for humanity — and, crucially, into infrastructure that can be put in the hands of local actors rather than reserved for states with their own satellites.

This shift moves PeaceTech from simply observing conflict to *enabling* it to be prevented: strengthening resilience, protecting civilians, supporting humanitarian operations, safeguarding critical infrastructure, improving environmental stewardship, and advancing **space-enabled health through disease monitoring and**

emergency medical connectivity. Together, these capabilities underpin international peace and security. The trend is visible across a widening set of domains:

- **Satellite democratization for local peacebuilders** [Emerging] — independent, community-tasked Earth-observation missions that let local communities monitor humanitarian crises, human-rights violations, and environmental destruction · *Common Space (founded 2025) — Kluz Prize 2025 winner*
- **Underground resource mapping to prevent scarcity conflict** [Emerging] — detecting groundwater and natural resources from orbit to reduce scarcity and prevent conflict · *Lunasonde AstroGPR groundwater detection — Kluz Prize 2024 distinction (Space Technology for Peace)*
- **Low Earth Orbit (LEO) constellations for real-time conflict watch** [Frontier] — LEO constellations delivering continuous monitoring through optical imagery, synthetic-aperture radar, and AI-powered analytics · *Planet Labs daily imagery*
- **Satellite direct-to-device connectivity for populations without internet access** [Frontier] — satellite communications and direct-to-device connectivity that maintain essential services during conflicts, disasters, and internet shutdowns · *Starlink/Kyivstar direct-to-cell in Ukraine (2025–26); Iran blackout workaround (2026)*
- **Satellite mapping of conflict zones** [Established] — the established baseline: UNOSAT's geospatial monitoring of conflict zones since 2001, the frontier is ongoing mapping of agricultural, forest, atmospheric, and water damage across conflict-affected countries and disseminating data responsibly to key actors · *UNOSAT geospatial monitoring (since 2001)*

Beyond these, an expanding space economy is generating dual- and triple-use capabilities with direct peace relevance — from **orbital AI and edge computing** that speeds disaster response, to **resilient positioning, navigation, and timing** that protects civilian logistics, to **space health, biotechnology, and in-space manufacturing** whose spillovers reach humanitarian medicine. The map below organizes the emerging space technology stack into five layers. As shown in the table below, the peace-and-security layer is related to PeaceTech, while the other layers create the infrastructure for these peace innovations.

Infrastructure	Earth observation · Satellite communications · Positioning, navigation & timing · Space-based data centres · Orbital AI & edge computing · Space weather · Space domain awareness · Space cybersecurity
Mobility	Reusable launch systems · Orbital logistics · In-space servicing & refuelling · Debris removal · Space transportation
Humanity	Space health · Space biotechnology · Space-enabled drug discovery · Microgravity manufacturing · Space agriculture & food systems · Life-support technologies
Exploration	Space exploration · Lunar infrastructure · Space resources (ISRU) · Space science
Peace & Security (PeaceTech)	Community-tasked satellites · Humanitarian satellite services · Disaster response · Environmental monitoring · Resource monitoring · Non-proliferation verification from space Space health

The peace-and-security layer is where space infrastructure becomes PeaceTech most directly; the other four layers supply the capabilities it runs on.

Investment Strategy. Invest in open, resilient, and internationally accessible space infrastructure and services that strengthen peace, protect human dignity, and serve humanity. Prioritize civilian applications, interoperability, transparency, and independent access while safeguarding against militarization. *(risk 2/5 · opportunity 5/5)*

Trend 4 — From "more data" to trustworthy data

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
Reliable, legitimate, safe data	Frontier; mostly still concepts	Data-governance bodies, funders, conflict-affected communities
RISK ●●○○○ *low direct-harm risk — the point is to reduce the surveillance risk other trends carry*	**OPPORTUNITY** ●●●●○ *the enabling layer for every other trend, and the least mature*	

The field has learned the hard way that abundant data is not the same as reliable, legitimate, or safe data. The trustworthy-data trend treats provenance, privacy, and data sovereignty as core PeaceTech infrastructure rather than afterthoughts — because in conflict settings, data collected to help people can be turned against them the moment institutions falter. This is one of the least mature but most consequential trends: much of it is still concept and pilot.

- **Verifiable provenance for conflict evidence (C2PA-type)** [Frontier] — verifiable provenance for conflict evidence, so a video can be authenticated for a tribunal — standards are emerging · *Bellingcat/GLAN/Mnemonic court-tested Yemen chain-of-custody; C2PA provenance standard*
- **Sovereign / trustworthy data commons for affected communities** [Frontier] — sovereign, trustworthy data commons that let conflict-affected communities govern information about themselves · *Data Collaboratives; Indigenous CARE data-governance principles*
- **Privacy-preserving analytics on conflict data** [Frontier] — privacy-preserving analytics on conflict data, via differential privacy and federated learning · *differential-privacy pilots for humanitarian research*
- **Confidential compute for sensitive humanitarian data** [Frontier] — confidential compute for sensitive humanitarian data, borrowed from enterprise and barely explored for peace · *ICRC data-protection work*

Investment Strategy. Fund data access as shared infrastructure (e.g. data commons), not project by project. *(risk 2/5 · opportunity 4/5)*

Trend 5 — From classical to quantum-era assumptions

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
Quantum security and sensing	Frontier; over the horizon	Researchers, long-horizon funders, conflict-affected communities
RISK ●●○○○ *no near-term peace-harm; the risk is the opportunity cost of premature investment*	**OPPORTUNITY** ●●○○○ *genuinely over the horizon — worth watching and seeding, not over-committing*	

Still mostly over the horizon, but no longer ignorable. Quantum technologies enter PeaceTech from two directions: security, where quantum-secured channels could protect mediators and aid coordination from interception, and sensing, where quantum magnetometry could detect subsurface ordnance that today's sensors cannot. None of this is deployed for peace yet — which is precisely why a benchmark report should start tracking it now, before the capability is defined solely by its military uses.

- **Quantum-secured communications for mediation & aid** [Frontier] — quantum-secured communications for mediation and aid flows, with no deployed peace application yet · *No deployed peace application; builds on national QKD networks (e.g. China, EU EuroQCI)*
- **Quantum sensing for subsurface UXO / tunnel detection** [Frontier] — quantum sensing for subsurface UXO and tunnel detection — a potential step-change for demining, at lab stage · *Quantum magnetometry research (e.g. Q-CTRL, university labs); lab-stage for demining*

Watch item: quantum and high-performance optimization of humanitarian logistics — routing and pre-positioning aid under uncertainty — is a plausible third application the field should monitor as hardware matures.

Investment Strategy. Track and make small seed bets; revisit each year. *(risk 2/5 · opportunity 2/5)*

Trend 6 — From digital-only to biosecurity

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
Biology as a peace-and-conflict domain	Frontier; high dual-use risk	Governments, WHO, biosecurity community, conflict-affected communities
RISK ● ● ● ● ● *offense-dominant and hard to attribute — the highest-risk category in this report, irreversible if it materializes*	**OPPORTUNITY** ● ● ● ● ○ *surveillance and verification are high-value, but only in equipped hands*	

Biotechnology is now recognised alongside AI as a defining emerging technology for peace and conflict. Genome editing, AI-driven protein design, and automated biofoundries lower the barriers to engineering biology — accelerating beneficial applications while making biological risk more diffuse and harder to attribute. This is the trend where the offense-defense balance is least favourable, so its peace-facing applications — surveillance, verification, resilience — matter disproportionately.

- **Pathogen surveillance & outbreak early warning in conflict zones** [Frontier] — pathogen surveillance and outbreak early warning in conflict zones, where health systems have collapsed · *WHO EIOS open-source outbreak intelligence; Nextstrain genomic surveillance*
- **Biosecurity verification for the Biological Weapons Convention** [Frontier] — biosecurity verification for the Biological Weapons Convention, which today has no deployed verification regime · *NTI | bio BWC transparency work; IBBIS (Geneva, launched 2024)*
- **AI screening of DNA synthesis orders** [Frontier] — AI screening of DNA synthesis orders, a cryptographic check against the misuse of synthesis · *IBBIS Common Mechanism (commec) — free open-source DNA-synthesis screening, launched 2024*
- **Food security & crop resilience in conflict-affected regions** [Frontier] — food security and crop resilience in conflict-affected regions, an under-developed peace framing of agri-biotech · *FAO/WFP crop monitoring; CGIAR climate-resilient seed programs in fragile states*

A note of caution. This trend carries a heavier governance burden than any other in this report. Engineered biological capability is hard to attribute and hard to defend against; work here demands more scrutiny, not less, and belongs only with actors equipped to contain it.

Investment Strategy. Fund only with containment capacity and independent oversight. *(risk 5/5 · opportunity 4/5)*

Trend 7 — From monitoring conflict to verifying restraint

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
Technology that makes agreements credible	Frontier; research to early use	Arms-control bodies, states, UN, conflict-affected communities
RISK ●●○○○ *constructive by design, with low misuse risk*	**OPPORTUNITY** ●●●●● *Makes agreements credible as arms control weakens*	

The Biological Weapons Gap Convention verification gap flagged in Trend 6 is precisely the frontier that verification technology in Trend 7 is best positioned to close. Verification technology is the constructive counterpart to defense technology, and it has advanced substantially: satellite and sensor networks for treaty monitoring, open-source verification by non-governmental analysts, and cryptographic methods that can authenticate a warhead or a dismantlement claim without revealing sensitive design information. As arms-control architecture weakens, the technical capacity to verify agreements becomes a precondition for rebuilding it — which makes this one of the highest-leverage trends in the report.

- **Cryptographic warhead authentication for disarmament** [Frontier] — cryptographic warhead authentication for disarmament, using zero-knowledge and physical-encryption methods · *Princeton / PPPL zero-knowledge warhead verification (Glaser & Goldston, Nature 2014; physical demo 2016), IAEA Safeguards, CTBTO's verification regime*
- **Open-source treaty & proliferation monitoring** [Frontier] — open-source treaty and proliferation monitoring by NGO analysts using commercial imagery · *Bellingcat Global Authentication Project; James Martin CNS open-source nonproliferation analysis*
- **Sensor networks for treaty compliance monitoring** [Frontier] — extending established test-ban monitoring to new arms-control regimes · *CTBT-style seismic/acoustic arrays; extension to new regimes*
- **ML-augmented arms-control inspection** [Frontier] — ML-augmented arms-control inspection, proposed to support inspectors but not yet authenticated for use · *IAEA machine-learning safeguards analysis*
- **Space-based non-proliferation compliance monitoring** [Emerging] — already emerging on commercial satellite infrastructure · *Humanitarian Research Lab (Yale University)*

Investment Strategy. High-return bet in this report. *(risk 2/5 · opportunity 5/5)*

Trend 8 — From technology for resource security to conflict prevention

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
Tech where scarcity drives violence	Emerging → frontier	Energy and natural resources funds, corporations, development actors, infrastructure providers, UN, conflict-affected communities
RISK ●●○○○ *low direct risk; the care needed is not to securitise humanitarian data*	**OPPORTUNITY** ●●●●○ *connects two large funded communities with a clear causal path to prevention*	

Where resource and infrastructure pressures contribute to conflict—through water shortages, food insecurity, displacement, competition over natural resources and critical minerals, or disruption to energy grids—the technologies used to anticipate and manage these risks can become PeaceTech.

- **Underground resource mapping to prevent scarcity conflict** [Emerging] — resource mapping from space (Lunasonde) again, this time read as scarcity prevention · *Lunasonde AstroGPR groundwater detection — Kluz Prize 2024 distinction (Space Technology for Peace)*
- **Tech-enabled transboundary water / resource co-management** [Frontier] — transboundary water and resource co-management, where agreements exist but the enabling technology is absent · *Nile Basin Initiative decision-support; OSU Transboundary Freshwater Dispute Database*

- **Water-stress early warning in transboundary basins** [Frontier] — water-stress early warning in transboundary basins, where scarcity meets contested borders · *Water, Peace & Security Partnership (WRI, IHE Delft, Pacific Institute); UN-led Nile/basin monitoring*
- **Climate-conflict risk forecasting** [Frontier] — climate-conflict risk forecasting, linking climate stress to the onset of violence · *Water, Peace & Security Partnership Global Early Warning Tool (~86% of conflicts captured)*
- **Displacement anticipation & planning** [Frontier] — displacement anticipation and planning, moving from reaction to anticipatory action · *IDMC displacement modelling; Red Cross Anticipatory Action / forecast-based financing*

Investment Strategy. Fund technologies that strengthen resource security and societal resilience; require a clear and measurable connection to conflict prevention. *(risk 2/5 · opportunity 4/5)*

Trend 9 — From vulnerable systems to resilient critical infrastructure

THE SIGNAL	WHERE IT STANDS	STAKEHOLDERS
Essential systems that keep working under pressure	Emerging; unevenly deployed	Governments, infrastructure operators, cities, development banks, humanitarians, conflict-affected communities
RISK ●●●○○ *resilience tools can also enable surveillance, centralised control, and dependence on private operators*	**OPPORTUNITY** ●●●●● *civilian survival, economic continuity, and social stability depend on essential systems staying operational*	

Conflict increasingly targets the systems on which civilian life depends: electricity, water, telecommunications, healthcare, transport, financial networks, cloud infrastructure, and public digital services. Cyberattacks are becoming increasingly commonplace, demonstrating the urgent need to improve threat intelligence sharing, incident response capacity, and overall cyber resilience. Critical-infrastructure PeaceTech moves beyond repairing these systems after destruction toward **designing them to anticipate disruption, operate under attack, recover rapidly, and keep serving communities when central institutions fail.**

This is not simply conventional infrastructure investment. It becomes PeaceTech when resilience is explicitly tied to protecting civilians, preventing social breakdown, limiting displacement, and reducing the chance that an infrastructure failure escalates into violence. The trend spans several fast-emerging capabilities:

- **Cyber-resilience for hospitals and humanitarian organisations** [Emerging] — systems that preserve healthcare, humanitarian beneficiary data and digital operations of aid agencies through ransomware, network disruption, or hostile cyber activity. *Halcyon research on ransomware in public health crises*
- **Distributed energy and microgrids** [Emerging] — decentralized energy that keeps hospitals, shelters, water facilities, and communications running when national grids fail. *Ukraine's cogeneration and decentralized solutions; WHO research on decentralized sustainable energy solutions*
- **Resilient water infrastructure and contamination monitoring** [Emerging] — sensor networks, decentralised purification, and rapid-response systems that protect water access during conflict or institutional collapse. *No deployed peace application; Planet Water Foundation's disaster response platform ensures water access after environmental disasters*
- **Digital public infrastructure continuity** [Frontier] — resilient identity, payments, benefits, and public-service systems that keep operating during displacement, occupation, or state fragmentation. *Ukraine's Diia Platform*
- **AI-enabled infrastructure failure prediction** [Frontier] — predictive-maintenance and digital-twin systems that find vulnerabilities in bridges, grids, pipelines, hospitals, and transport before catastrophic failure. *No deployed peace application: Oxmaint AI: predictive maintenance for critical infrastructure*

- **Rapidly deployable communications and computing** [Emerging] — portable cloud, edge computing, mesh, and satellite-enabled systems that restore essential services after infrastructure loss. *No deployed peace application; Hughes Network Systems: disaster response communications*
- **Resilient financial and payment infrastructure** [Frontier] — continuity tools that let households, humanitarian agencies, and local businesses transact when banking or connectivity is disrupted. *No deployed peace application; research on payment resilience in conflict-affected states*

Investment Strategy. Fund as essential civilian-protection infrastructure; require interoperability, local ownership, cyber-security, and safeguards against the misuse of sensitive data. . *(risk 3/5 · opportunity 5/5)*

Two cross-cutting enablers

Two capabilities run through all nine trends and deserve their own mention. **Resilient communications** such as mesh networks, satellite direct-to-device, and offline-first protocols matter because communications blackouts are now a standard instrument of conflict. Every tool in this report assumes connectivity that is often the first thing to disappear.

- **Mesh & offline-first comms under blackout conditions** [Frontier] — mesh and offline-first communications under blackout conditions, deployed ad hoc but not yet standard infrastructure · *Meshtastic; Bridgefy during protest blackouts (Hong Kong,)*
- **Satellite direct-to-device connectivity for populations without internet access** [Frontier] — satellite direct-to-device connectivity for cut-off populations, with commercial rollout just beginning · *Starlink/Kyivstar direct-to-cell in Ukraine (2025–26); Iran blackout workaround (2026)*

And the field's own missing tooling. The trends above generate capability; the field still lacks the instruments to govern and evaluate it. This is the least glamorous and arguably most urgent gap.

- **PeaceTech impact-measurement & evaluation frameworks** [Frontier] — PeaceTech impact-measurement and evaluation frameworks — largely absent, and the precondition for knowing what works · *Alliance for Peacebuilding evaluation standards (largely nascent)*

4. How to judge the frontier

Frontier technologies can serve commercial and civilian needs, advance peace and human security, or be adapted for conflict, coercion and harm. Their impact therefore depends not only on what is built, but also on who deploys it, for what purpose and under what safeguards.

The below framework is used to assess each of the nine trends in the risk-and-opportunity matrix at the end of the report, connecting technological judgment with investment decisions.

The Peace Dividend Test

The defining characteristic of PeaceTech is not technological sophistication but **measurable societal benefit.** A genuine PeaceTech application should demonstrate a credible peace dividend — a concrete contribution to one or more of the following:

- **Saving lives**: helping to reduce death and injury in conflict and crisis
- **Preventing violence**: heading off escalation before it turns lethal
- **Protecting civilians**: shielding non-combatants and the displaced from harm
- **Reducing human suffering**: easing the humanitarian toll of conflict
- **Strengthening humanitarian response**: making relief faster, safer, and better-coordinated
- **Rebuilding trust**: restoring the relationships and institutions conflict destroys
- **Strengthening resilient societies**: hardening the systems on which peaceful life depends
- **Safeguarding human dignity**: keeping the human person at the centre of every application
- **Ethical oversight:** using independent, multi-stakeholder mechanism ensures ongoing accountability

It is important to note that dual and triple-use applications are particularly challenging to assess and must be evaluated with extreme caution.

To separate a real peace dividend from a marketed one, every technology should be able to answer five questions:

- **Outcome** — What measurable peace outcome does it create?
- **Beneficiary** — Who benefits — and who is excluded?
- **Measurement** — How will that impact be measured over time?
- **Evidence** — What evidence supports the claim today?
- **Net effect** — Could misuse outweigh the expected benefit?

5. The investment case

The largest challenge facing PeaceTech is not technical. It is that the field is starved of money and saddled with a perception problem, and the two reinforce each other. For the funders and investors this report addresses, that is not a reason for caution — it is the opportunity, and it is largest in exactly the trends the above sections identified.

The numbers

The economic impact of violence reached roughly $21.8 trillion USD in 2025 — 10.5% of global GDP — and global military expenditure increased by roughly 5% in 2025. Against that, spending on peacebuilding and peacekeeping was $49.2 billion USD in 2025 which is roughly 0.5% of dollars spent on military globally. Capital is flowing to the tools of war and away from the tools of prevention — precisely as conflicts multiply.

The capital landscape

Different PeaceTech technologies require different forms of capital. Some applications are well suited to venture investment; others depend on government procurement, development finance, philanthropy, or public–private partnerships. A demining-robotics company can raise a venture round; a biosecurity-verification protocol or a sovereign data commons may never fit a venture return profile and instead needs patient public or philanthropic money. Matching the financing model to the technology is essential if frontier innovations are to move beyond research and pilots into large-scale deployment — and mismatching it is one of the quiet reasons promising PeaceTech stalls.

The objection we take seriously

There is a serious critique of everything argued here. Researchers call it the **visibility paradox**: the field now has unprecedented tools for prediction, mapping, and monitoring, yet greater visibility does not reliably produce decisive preventive action. On this reading PeaceTech is "new wine in old bottles," genuine innovation running into the same political-will constraints that have always limited conflict prevention.

We think this is largely right, and that it sharpens rather than defeats the case. It means the binding constraint is often not sensing but *acting* — and that funding yet another forecasting model may add little. It is an argument for directing capital to the parts of the frontier that attack the bottleneck: decision-support integrated into real workflows, verification and accountability tooling that raises the cost of inaction, and the impact measurement that would let anyone tell what works. Notably, that is exactly the normative and operational tooling the field has least of. The critique and the funding gap point the same way.

The "soft" problem and the triple-use answer

Underneath the funding gap is a **connotation problem**. "Defense" — or, more bluntly, war technology — reads as serious and strategic; "peace" reads as soft and charitable, a cost centre rather than a capability. It is worth stating plainly: preventing a war is one of the highest-return, hardest-nosed things a technology can support. One way to move past this divide is **triple-use technology** — technology that delivers a genuine peace dividend alongside commercial and defense applicability.

The technologies shaping the next decade increasingly create value across three domains at once: **commercial markets, defense, and peace.** Rather than treating these as competing objectives, PeaceTech recognizes the emergence of triple-use technologies — innovations that can generate economic value, strengthen security, and deliver measurable benefits for peace. Many of the frontier technologies in this report such as artificial intelligence, robotics, satellite and space infrastructure, trusted data, biotechnology, resilient communications, and critical infrastructure are inherently triple-use. Their societal impact depends not on the technology itself but on governance, incentives, and intended outcomes.

The challenge for entrepreneurs, investors, policymakers, and governments is therefore not whether a technology is dual- or triple-use, but **whether its peace dividend is intentionally designed, measured, governed, and rewarded** alongside its commercial and security value. Recognizing and investing in triple-use technologies is an opportunity to align innovation, prosperity, security, and peace rather than trading one against another — but only where the peace dividend is real and tested against the Peace Dividend Test above, not merely asserted.

The missing middle

Many PeaceTech innovations demonstrate technical feasibility but fail before reaching operational deployment. The largest funding gap lies not at the research stage but **between prototype and adoption** — the "missing middle" where a working pilot needs a first customer, a certification, a procurement contract, and the patient capital to survive the years before scale. Closing it means funding pilots, procurement, certification, first-customer programs, and long-term institutional adoption alongside the technology itself. For most of the frontier trends in this report, the missing middle — not the science — is the binding constraint.

What we are asking

A call to the field

- **Fund the frontier.** Direct capital toward the nine trends, with a dedicated PeaceTech fund and a deliberate focus on triple-use technologies.
- **Invest with a test, not a slogan.** Apply Peace Dividend Test to every commitment, so that "PeaceTech" in a portfolio means something.
- **Recognize and de-risk early work.** Use prizes, accelerator access, mentorship, and pilots to move frontier tools from concept to deployment.
- **Build shared infrastructure.** Back the connective tissue including governance, measurement standards, and a common tech stack for conflict-affected regions that no single tool will fund but the whole field needs.

Where the opportunity concentrates. Opportunity is highest in **verification technology** and **space infrastructure** — high-leverage, maturing, and badly under-funded — followed by **trustworthy data**, **climate-security**, **agentic AI**, **autonomous robotics**, and **biosecurity**. It is lowest, for now, in **quantum-era** tools that remain over the horizon. Those per-trend opportunity scores are the horizontal axis of the matrix that follows.

6. The risk–opportunity matrix

This matrix plots each of the nine trends by its **risk** against its **opportunity**. The quadrants translate directly into funding posture: high opportunity with manageable risk is where capital should move first; high opportunity with high risk needs capital plus containment; low opportunity is where to watch rather than commit.

	Lower opportunity	Higher opportunity
Higher risk	**Watch / contain** — *Low upside, real risk — deprioritise.*	**Fund with containment** • Agentic AI (4/4) • Autonomous & swarm robotics (4/4) • Biosecurity (5/4) *High upside, high risk — invest plus oversight.*
Lower risk	**Watch / seed** • Quantum-era (2/2) *Low upside for now — track, seed lightly.*	**Fund first** • Space infrastructure (2/5) • Trustworthy data (2/4) • Verification tech (2/5) • Climate-security (2/4) • Resilient critical infrastructure (3/5) *High upside, manageable risk — move capital here first.*

Position reflects the per-trend risk and opportunity scores introduced with each trend. Scores are the report's own judgment, meant as a starting point for a funder's due diligence, not a substitute for it.

The verdict on each trend

Trend	Risk	Opp.	Funding verdict
Verification tech	2	5	The clearest under-funded, high-return bet in this report.
Space infrastructure	2	5	Invest now; prioritise independent, community-tasked capacity.
Resilient critical infrastructure	3	5	Fund as essential civilian-protection infrastructure; require interoperability, local ownership, cyber-security, and safeguards against surveillance.
Trustworthy data	2	4	Fund as shared infrastructure, not project by project.
Energy-security	2	4	Fund at the energy and climate peace seam; insist on the causal test.
Agentic AI	4	4	Fund with strong human-in-the-loop and audit requirements.
Autonomous & swarm robotics	4	4	Back demining-specific applications; ring-fence against weaponisation.
Biosecurity	5	4	Fund only with containment capacity and independent oversight.
Quantum-era	2	2	Track and make small seed bets; revisit each year.

Reflection: The future of technology must serve humanity

Technological progress is not measured solely by greater capability but by whether it advances the dignity of every person and contributes to authentic human flourishing.

The technologies described throughout this report will undoubtedly become more powerful. The more important question is whether they strengthen peace, freedom, justice, solidarity, and the common good —

or whether they deepen conflict, inequality, and human vulnerability. That question is not answered by the technology; it is answered by the choices made around it.

PeaceTech begins with the conviction that innovation is not an end in itself. Its highest purpose is to serve humanity.

The choice

The frontier technologies in this report are being built regardless. The only open question is whether they are pointed toward deepening conflict or toward more dignified, inclusive, and resilient societies. That is a choice — and, more than anything else, a choice about where capital and attention go. **The technology will arrive on its own. Whether it serves peace will not.**

7. The next decade: PeaceTech in 2035

Plausible field destinations

If the nine trends in this report mature and the missing middle is funded, the shape of the field a decade out becomes possible to sketch. None of the following is a prediction; each is a plausible destination that today's frontier already points toward:

- **Agentic mediation** — AI systems that routinely help human mediators surface options and blind spots in live negotiations
- **Autonomous humanitarian logistics** — self-coordinating fleets delivering aid and clearing hazards at scale
- **Global verification infrastructure** — a standing technical capacity to verify arms-control and ceasefire commitments
- **Space infrastructure serving humanity** — open, resilient orbital systems underpinning humanitarian response worldwide
- **Trusted AI governance** — mature standards, audits, and oversight for AI used in conflict settings
- **Planetary-scale disaster response** — real-time, space- and AI-enabled coordination across borders
- **Critical-infrastructure resilience** — civilian systems designed from the outset to survive conflict and disaster
- **New international institutions** — governance bodies built for frontier technologies rather than retrofitted to them

Which of these arrive, and whether they serve peace, will depend less on the technology than on the decisions the readers of this report make in the years between now and then.

Technologies to watch

Beyond the nine trends sit capabilities that are not yet PeaceTech but could become decisive — for peace or against it — within the next few years. We track them here so that each edition can register the moment they cross from possibility into practice. They fall into two clusters: general-purpose breakthroughs, and the fast-expanding space economy.

General-purpose breakthroughs

▹ Brain–computer interfaces	▹ Synthetic media	▹ General-purpose humanoid robotics
▹ Advanced materials	▹ Fusion energy	▹ Synthetic biology
▹ Autonomous scientific discovery	▹ AI scientists	▹ Digital twins of societies

The expanding space economy

▹ Commercial space stations & orbital economies	▹ Space-based solar power	▹ In-space manufacturing
▹ Orbital data centres & cloud	▹ Cislunar infrastructure & logistics	▹ Space traffic management
▹ Planetary defense & NEO protection	▹ Lunar & asteroid ISRU	▹ Advanced reusable orbital transport
▹ Autonomous space robotics & on-orbit servicing	▹ Interplanetary comms & navigation	

8. The 100 use cases: full index

The complete catalogue underpinning this report. Each use case is tagged by conflict phase, primary technology, dimension (technical / operational / normative), and maturity tier. Entries marked with a Prize year were recognized by the Kluz Prize for PeaceTech.

Established · 30	Emerging · 31	Frontier · 39

Established (30)

#	Use case	Example / evidence	Phase
1	**3D printing for infrastructure rebuild**	Team4UA / COBOD 3D-printed school, Lviv	Post-conflict
2	**AI-enabled UXO / landmine detection**	UNOPS Compass toolkit (Ukraine) — Kluz Prize 2025 distinction (International Organization Advancing Peace)	Post-conflict
3	**Antisemitic hate-speech crowdsourced reporting**	HO:PE (World Jewish Congress / EU)	Pre-conflict
4	**Big-data tracking of conflict incidents**	#DataforUkraine (events 3-7 hrs faster than media)	During conflict
5	**Blockchain for transparent aid disbursement**	WFP Building Blocks (Syria, Palestine)	During conflict
6	**Ceasefire monitoring via satellite + AI**	Hala Systems 'Sentry' (Yemen)	Post-conflict
7	**Collaborative dialogue platform for mediators**	Inclus (Europe, MENA, Asia, Africa)	During conflict
8	**Community alert apps for local monitoring**	AlertMe (1,908 incidents, South Sudan)	During conflict
9	**Conflict early-warning forecasting**	VIEWS (PRIO/Uppsala); GCRI (EU JRC), 138 countries — Kluz Prize 2024 distinction (Use of AI for Peace)	Pre-conflict
10	**Cross-border predictive early warning**	IGAD CEWARN (East Africa, since 2002)	Pre-conflict
11	**Crowdsourced incident reporting**	Ushahidi; AlertMe (South Sudan)	During conflict
12	**Digital civic-participation dialogues**	Guatemala Joven Conversa (900 youth)	Long-term peacebuilding
13	**Digital identity for service access**	Estonia e-ID	Long-term peacebuilding
14	**Digital refugee services & border coordination**	Commit Global (1.4M Ukrainian refugees) — Kluz Prize 2023 winner	During conflict
15	**Drone delivery of medical supplies**	Draganfly (Ukraine frontlines, 35 lb payload)	During conflict
16	**Drone-based demining**	Aerobotics7 EAGLE A7 (Ukraine) — Kluz Prize 2024 winner	Post-conflict
17	**Evidence collection for human-rights accountability**	UN Fact-Finding Mission on Iran (38,000+ items)	During conflict
18	**Game-based peace education**	Minecraft Peace Builders (40,000 schools, 140 countries)	Long-term peacebuilding
19	**Humanitarian aid coordination on shared ledger**	UN WFP Building Blocks (4.8M households; 159 orgs)	During conflict
20	**Online peace-education courses**	edX UNESCO; Coursera diplomacy (Univ. of London)	Long-term peacebuilding
21	**Open-source mapping for humanitarian response**	Humanitarian OpenStreetMap Team (Sudan diaspora mapping) — Kluz Prize 2025 distinction (Open Source Technology)	During conflict
22	**Peace education & community dialogue programming**	Magnolia Foundation, School of Peace (Colombia) — Kluz Prize 2022 winner	Long-term peacebuilding
23	**Rumour fact-checking via SMS**	Kijiji Cha Amani (DRC), Sentinel Project	Pre-conflict
24	**Satellite damage assessment of heritage sites**	UNOSAT Sudan cultural-heritage documentation	During conflict
25	**Satellite mapping of conflict zones**	UNOSAT geospatial monitoring (since 2001)	During conflict

#	Use case	Example / evidence	Phase
26	**Social-media hate-speech detection**	TrollWall AI (12 languages, EU elections)	Pre-conflict
27	**Statistical estimation of human-rights violations**	HRDAG, Colombia Truth Commission (112 datasets) — Kluz Prize 2023 distinction	Post-conflict
28	**Structured humanitarian data analysis across agencies**	DEEP platform, Danish Refugee Council — Kluz Prize 2024 distinction (Humanitarian Impact)	During conflict
29	**VR empathy building / war memory**	'War Remains', US National WWI Museum	Long-term peacebuilding
30	**VR psychotherapy for conflict-related PTSD**	Virtual Ukraine Project	Post-conflict

Emerging (31)

#	Use case	Example / evidence	Phase
31	**AI analysis of propaganda / influence operations**	Stanford Internet Observatory; EU DisinfoLab; DFRLab influence-operation tracking	Pre-conflict
32	**AI conflict-ripeness analysis for negotiations**	Project Didi (Israel/Palestine media analysis) — Kluz Prize 2023 distinction (Innovative Use of AI/ML)	During conflict
33	**AI counter-narrative content curation**	Moonshot CVE; Jigsaw Redirect Method (EU/US P/CVE deployments)	Long-term peacebuilding
34	**AI electoral-integrity monitoring**	The Carter Center election observation tech; Democracy Reporting International social-media monitoring	Pre-conflict
35	**AI peace-scenario modelling**	CSIS Futures Lab Ukraine scenarios (RAG)	During conflict
36	**AI seafloor / environmental cleanup**	SEACLEAR 2.0 (EU-funded)	Long-term peacebuilding
37	**AI translation for asylum & legal processes**	Tarjimly (refugee interpretation app); RESPOND / Lighthouse legal-aid translation pilots	Post-conflict
38	**Agentic AI geopolitical simulation**	Anadyr Horizon decision-maker modelling — Kluz Prize 2025 distinction (Use of AI for Peace)	Pre-conflict
39	**Automated ceasefire-violation detection**	Hala Systems 'Sentry' (Yemen); Ceasefire monitoring via PlanetScope + AI event detection	Post-conflict
40	**Blockchain identity for stateless / displaced persons**	UNHCR Stellar/USDC wallets (Ukraine); WFP Building Blocks self-sovereign ID (Jordan, Bangladesh)	During conflict
41	**Community transparency / accountability trackers**	ICE Activity Tracker (US crowdsourcing)	During conflict
42	**Crowdsourced constitutional / peace-process design**	Iceland crowdsourced constitution (analogue)	Long-term peacebuilding
43	**Deepfake detection for conflict disinformation**	WITNESS 'Prepare, Don't Panic'; Intel FakeCatcher; UNHCR flagging deepfakes of aid staff	Pre-conflict
44	**Digital public infrastructure for fragile states**	MOSIP open-source ID (Morocco, Philippines, Ethiopia); GovStack DPI framework	Post-conflict
45	**Digital truth & reconciliation platforms**	Colombia JEP / Truth Commission digital archives; HRDAG-supported case systems	Post-conflict
46	**Digital twins for negotiation-outcome modelling**	CulturePulse ARES (UNDP; Palestine, Balkans)	During conflict
47	**Digitised reparations / transitional-justice registries**	Colombia JEP digital systems	Post-conflict
48	**Empathy-building agentic AI between opposing groups**	Stanford Peace Innovation Lab; MIT/Harvard 'AI mediation' study (Nature 2024)	Long-term peacebuilding
49	**Environmental damage assessment in conflict**	UNEP / satellite-based post-strike pollution monitoring	Post-conflict
50	**Federated data sharing across humanitarian orgs**	Centre for Humanitarian Data (OCHA); Building Blocks multi-agency ledger (17 orgs, Beirut)	During conflict

#	Use case	Example / evidence	Phase
51	**LLM blind-spot identification in negotiations**	Belfer Center research on AI and conflict resolution; CSIS Futures Lab	During conflict
52	**Multilingual AI for mediation across languages**	Carnegie / UN University multilingual AI	During conflict
53	**Open-source arms-trade tracking**	SIPRI Arms Transfers Database; Trade Data Monitor + OSINT analysis	Pre-conflict
54	**Satellite democratization for local peacebuilders**	Common Space (founded 2025) — Kluz Prize 2025 winner	During conflict
55	**Satellite monitoring of conflict resource extraction**	Global Witness conflict-mineral tracking; Global Forest Watch adapted for conflict zones	Pre-conflict
56	**Space-based non-proliferation compliance monitoring**	Commercial satellite approaching this	Pre-conflict
57	**Trauma-informed AI for survivor testimony**	USC Shoah Foundation Dimensions in Testimony; WITNESS survivor-documentation guidance	Post-conflict
58	**Underground resource mapping to prevent scarcity conflict**	Lunasonde AstroGPR groundwater detection — Kluz Prize 2024 distinction (Space Technology for Peace)	Long-term peacebuilding
59	**VR cross-community contact experiences**	Experimental Israeli-Palestinian encounters	Long-term peacebuilding
60	**VR training for peacekeeping personnel**	SkillDrill (Austrian Institute of Technology)	Pre-conflict
61	**Youth tech-peace hackathons**	Tech2Peace (Israeli & Palestinian youth)	Long-term peacebuilding

Frontier (39)

#	Use case	Example / evidence	Phase
62	**AI audit tools for bias & peacewashing detection**	Proposed (this report); adjacent: Ada Lovelace Institute / AlgorithmWatch auditing methods	Long-term peacebuilding
63	**AI screening of DNA synthesis orders**	IBBIS Common Mechanism (commec) — free open-source DNA-synthesis screening, launched 2024	Pre-conflict
64	**AI social-cohesion trend analysis**	UNDP social-cohesion analytics; Build Up 'The Commons' polarization research	Long-term peacebuilding
65	**AI translation for low-resource / indigenous peace processes**	Major NLP gaps for low-resource languages	During conflict
66	**AI-assisted peace-treaty drafting & gap analysis**	PA-X Peace Agreements Database (Edinburgh) + LLM analysis; Lex Machina-style legal AI	During conflict
67	**AI-enabled community reconciliation matching**	Concept; adjacent: Soliya / Search for Common Ground cross-community dialogue platforms	Post-conflict
68	**Agentic AI multi-party dialogue facilitation**	No large-scale deployment yet	During conflict
69	**Autonomous ground robotics for UXO clearance**	HALO Trust Ukraine R&D; Draganfly/Autonome Labs demining mesh; IOS/CMAC DMR robot	Post-conflict
70	**Biosecurity verification for the Biological Weapons Convention**	NTI | bio BWC transparency work; IBBIS (Geneva, launched 2024)	Pre-conflict
71	**Climate-conflict risk forecasting**	Water, Peace & Security Partnership Global Early Warning Tool (~86% of conflicts captured)	Pre-conflict
72	**Climate-displacement anticipation & planning**	IDMC displacement modelling; Red Cross Anticipatory Action / forecast-based financing	Pre-conflict
73	**Confidential compute for sensitive humanitarian data**	ICRC data-protection work; enterprise TEEs (Azure/AWS confidential compute) piloted for aid	During conflict
74	**Cryptographic warhead authentication for disarmament**	Princeton / PPPL zero-knowledge warhead verification (Glaser & Goldston, Nature 2014; physical demo 2016)	Post-conflict

#	Use case	Example / evidence	Phase
75	**Digital twins of cities for post-conflict rebuilding**	UN-Habitat reconstruction planning; digital-twin pilots for Mosul / Ukraine rebuilding	Post-conflict
76	**Food security & crop resilience in conflict-affected regions**	FAO/WFP crop monitoring; CGIAR climate-resilient seed programs in fragile states	Long-term peacebuilding
77	**Immersive empathy training for security forces**	SkillDrill-adjacent; not at scale	Pre-conflict
78	**ML-augmented arms-control inspection**	VERTIC verification research; IAEA machine-learning safeguards analysis	Pre-conflict
79	**Mesh & offline-first comms under blackout conditions**	Meshtastic; Bridgefy during protest blackouts (Hong Kong, Iran)	During conflict
80	**Open models & digital public goods for conflict-affected states**	Sovereignty alternative to vendor dependence	Long-term peacebuilding
81	**Open-source treaty & proliferation monitoring**	Bellingcat Global Authentication Project; James Martin CNS open-source nonproliferation analysis	Pre-conflict
82	**Pathogen surveillance & outbreak early warning in conflict zones**	WHO EIOS open-source outbreak intelligence; Nextstrain genomic surveillance	Pre-conflict
83	**PeaceTech impact-measurement & evaluation frameworks**	DfID/USIP evidence reviews; Alliance for Peacebuilding evaluation standards (largely nascent)	Long-term peacebuilding
84	**Persistent LEO constellations for real-time conflict watch**	Planet Labs daily imagery; Maxar & commercial LEO used by UN and journalists	During conflict
85	**Personalised counter-radicalisation AI**	Moonshot CVE Redirect campaigns; Jigsaw (early P/CVE research, not at scale)	Pre-conflict
86	**Predictive modelling of peace-agreement spoilers**	PA-X + PRIO research on spoiler dynamics (theoretical; not operationalised)	Post-conflict
87	**Predictive supply-chain analytics for humanitarian pre-positioning**	WFP Optimus logistics optimisation; IFRC pre-positioning analytics	Pre-conflict
88	**Privacy-preserving analytics on conflict data**	OCHA/UN Global Pulse differential-privacy pilots; federated-learning humanitarian research	During conflict
89	**Quantum sensing for subsurface UXO / tunnel detection**	Quantum magnetometry research (e.g. Q-CTRL, univ. labs); lab-stage for demining	Post-conflict
90	**Quantum-secured communications for mediation & aid**	No deployed peace application; builds on national QKD networks (e.g. China, EU EuroQCI)	During conflict
91	**Real-time mapping of group marginalisation**	Minority Rights Group data; Early Warning Project (Dartmouth/USHMM) — research stage	Pre-conflict
92	**Satellite RF / SAR monitoring of displacement at night**	ICEYE & Capella SAR; NASA Black Marble night-lights for displacement analysis	During conflict
93	**Satellite direct-to-device connectivity for cut-off populations**	Starlink/Kyivstar direct-to-cell in Ukraine (2025–26); Iran blackout workaround (2026)	During conflict
94	**Sensor networks for treaty compliance monitoring**	CTBT-style seismic/acoustic arrays; extension to new regimes	Pre-conflict
95	**Sovereign / trustworthy data commons for affected communities**	Data-collaborative models; Indigenous CARE data-governance principles	Long-term peacebuilding
96	**Swarm drones for large-scale demining**	HALO Trust AI-drone mapping (Ukraine); research on coordinated UAV clearance fleets	Post-conflict
97	**Tech-enabled transboundary water / resource co-management**	Nile Basin Initiative decision-support; OSU Transboundary Freshwater Dispute Database	Long-term peacebuilding
98	**Underwater autonomous vehicles for marine demining**	GICHD-tracked marine ROV trials; naval mine-hunting AUVs adapted for humanitarian use	Post-conflict
99	**Verifiable provenance for conflict evidence (C2PA-type)**	Bellingcat/GLAN/Mnemonic court-tested Yemen chain-of-custody; C2PA provenance standard	Post-conflict

#	Use case	Example / evidence	Phase
100	**Water-stress early warning in transboundary basins**	Water, Peace & Security Partnership (WRI, IHE Delft, Pacific Institute); UN-led Nile/basin monitoring	Pre-conflict

The Kluz Prize for PeaceTech Annual Frontier Report will track how these use cases mature — and which new ones emerge — in each subsequent edition.