Tech for Victims of Terrorism

2026 Working Groups

The United Nations Office of Counter-Terrorism (UNOCT) has launched a global call for nominations for its 2026 multisectoral Working Groups under the Tech for Victims of Terrorism initiative.

Bringing together participants from across sectors and regions, these Working Groups will help shape how new and emerging technologies can better support victims and survivors of terrorism. Their engagement will contribute to the development of a new Toolkit for Technology-Enabled Support to Victims of Terrorism, establishing a clear path for safe, responsible, and victim-centred digital innovation.

To drive this initiative forward, working groups will explore the following five challenges and opportunities:

- How to co-design digital tools with victims of terrorism and affected communities;
- How to design multilingual and culturally adaptive tools to support victims of terrorism;
- How to design for victims of terrorism in low-connectivity and low-resource contexts;
- How to ensure the safety and security of data relating to victims of terrorism in connected systems;
- How to create a safer internet for victims of terrorism.

1. Trauma-informed approaches for co-designing digital tools with victims of terrorism

Problem Statement

Many tools for communities in crisis are built *for* survivors rather than *with* them. This misses an opportunity to benefit from the lived experiences and expertise of victims of terrorism to co-create tools that are safe, used, and useful. Finding ways to co-design tools with the individuals and communities most affected by terrorism safely, respectfully, and effectively is essential to improving digital support services offered by governments, service providers, industry, and non-governmental organizations.

Toward Community-Led Design

As discussed in the Gap Analysis of Digital Tools to Support Victims of Terrorism, both the humanitarian and the tech sectors are increasingly recognizing the need to move beyond simple "user testing" and toward Community-Led Design. This shift recognizes that participation is a prerequisite for success and a potential pathway to healing for beneficiaries. There is a spectrum of possible engagement, from user-centered design to full co-production. Traditional standards, such as the SAMHSA principles of trauma-informed care (safety, trust, and peer support), remain relevant and can be adapted into frameworks for the design, development, deployment, and evaluation of digital tools.

Core Questions for the Working Group

To establish a roadmap for trauma-informed, integrated design, this working group will address questions such as:

- What are some shared elements and considerations for "inclusive co-design" that are trauma-informed and victim-centric?
- What are the main barriers to co-design with individuals and communities affected by terrorism, and how can these be overcome?
- How do we protect participants who are victims of terrorism from further trauma or harm throughout the tool design process?
- What standards and considerations should guide developers seeking to integrate victims' voices into different phases of the product design cycle, including problem definition, scoping and design, development and testing, and launch and governance?

2. Multilingual and culturally adaptive tools for victim support

Problem Statement

The broad reach and impact of any tool designed to support victims of terrorism depends on its multicultural fluency in grief and trauma as well as its availability in multiple languages. The under-representation of minority languages and communities in the Global South in the digital corpus used to train Large Language Models (LLMs) has knock-on effects on AI-enabled tools' ability to serve these populations safely and effectively. This is a problem larger than translation alone, and points towards structural limitations in ways in which these tools capture cultural context, social norms and other sensitive cues. Addressing these gaps requires investment in the development and training of AI-enabled models that are better equipped to engage in with linguistic diversity and cultural nuance, particularly in contexts involving trauma, vulnerability and the specific needs of victims of terrorism from around the world.

The State of Multicultural AI-enabled Tools

As discussed in the Gap Analysis of Digital Tools to Support Victims of Terrorism, relevant work is already underway to move from translation to cultural fluency. While models like Cohere's Aya have expanded support to 101 languages, initiatives like Google's Amplify demonstrate that technical capability must be paired with domain expertise to catch localized harms like misinformation or culturally specific triggers. Benchmarks, such as WorldView-Bench and CARE, allow developers to evaluate how models navigate conflicting global perspectives. Furthermore, architectures like Cultural Mixture of Adapters (CuMA) are being developed to prevent models from "averaging out" cultural values. National applications, such as India's Jugalbandi, show that government investment in specialized translation layers can be combined with generative AI to deliver vital information via accessible messaging platforms like WhatsApp.

Core Questions for the Working Group

To translate these research advancements into functional tools for victims of terrorism, this working group will address questions such as:

- How can we evaluate an AI-enabled system's ability to recognize and respond to "trauma cues" across different languages and cultural contexts?
- How can we fix pre-training, training, and reinforcement learning to ensure that diverse cultural or social values are reflected in the final model?
- How can we collect multicultural training data on trauma and grief in a way that is human rights-compliant, safe, trauma-informed and victim-centric?
- How can governments develop and support translation infrastructure for their national and minority languages, and how can the private sector build services on top?
- How do we implement "red-teaming" protocols that use local domain experts to test the safety and cultural relevance of AI-driven tools before they are deployed in high-stakes environments?
- How can we ensure that a human rights-based approach informs the design, development and use of relevant tools?

3. Designing for victims of terrorism in low-connectivity and low-resource contexts

Problem Statement

Digital tools are often designed for ideal conditions - high bandwidth, stable power, and high-spec hardware. For victims of terrorism in the Global South and rural areas, as well as many crisis scenarios where internet and power may shut down temporarily, these assumptions do not reflect reality. When connectivity is intermittent and energy is scarce, a text-heavy, high-data app isn't just inefficient; it is inaccessible. To bridge the digital divide, we must treat low bandwidth not as a bug to be fixed, but as a core design feature. Failure to account for these structural realities heightens the risk that the most vulnerable populations remain the least served.

Local Realities and Technical Resilience

As discussed in the Gap Analysis of Digital Tools to Support Victims of Terrorism, effective tools must be grounded in local realities. This requires a shift toward "low-tech" channels like SMS, USSD, and voice hotlines that function on basic feature phones. For web-based tools, "graceful degradation", where content loads gradually and functions offline or on-device, is essential. Practically, this also means prioritizing the design of tools to assist non-expert service providers such as community workers and designing for a wide range of accessibility challenges including low literacy. Ensuring that there is a digital tool offering that works in low-connectivity and low-resource environments – either through standalone tools or tools with offline or hybrid capabilities – is essential to ensure that we bridge rather than widen the digital divide.

Core Questions for the Working Group

To ensure digital tools are resilient enough for the most challenging environments, this working group will address questions such as:

- How do we provide complex services in low-data formats like USSD or SMS without losing the necessary nuance and safety?
- What are the design requirements for tools that allow non-specialist community workers to deliver evidence-based support safely and effectively, without a large cohort of expert care providers or government services to support them?
- How can we integrate audio, pictorial guidance, and voice options to support users with varying literacy levels and accessibility constraints?
- What are good practices for "offline-first" and “on-device” design that allows victims to access vital tools during connectivity blackouts?
- How do we build for capable on-device performance in traditionally high compute tasks such as translation and speech recognition?

4. Ensuring the safety and security of data relating to victims of terrorism in connected systems

Problem Statement

Digital connectivity can be a double-edged sword for victims of terrorism. While integrated digital victim registries and referral systems are essential for providing joined-up services, they carry risks. A data breach is rarely just a technical failure; it can result in serious and, in some cases, irreversible harm through the unauthorized disclosure of personal or sensitive information. Such harm may include re-traumatization, exposure to physical or security risks. In the absence of widely agreed standards for data handling, robust audit mechanisms, and clear accountability frameworks, trust in digital systems is difficult to establish, and well-intentioned technological solutions may inadvertently cause more harm than benefit.

Toward secure victim registries

As discussed in the Gap Analysis of Digital Tools to Support Victims of Terrorism, an international discussion is emerging on greater information connectivity and integrated digital services, for example through Digital Public Infrastructure (DPI). One use-case we explore in our analysis is developing Digital Victim Registries that can work with Digital ID and Data Exchange to allow victims to access multiple services without the need to re-authenticate or repeatedly "re-tell" their stories to different providers. Combined with privacy-by-design techniques like homomorphic encryption and metadata-only on-chain storage, these systems could allow for secure, auditable, and victim-controlled data sharing. If tools are designed from the outset to meet court-admissible evidentiary standards for the collection, handling and storage of data, these victim registries could also help support access to justice, including by contributing to criminal justice proceedings, subject to appropriate safeguards for privacy and data protection.

Core Questions for the Working Group

To build a secure and trustworthy digital architecture for the data of victims of terrorism, this working group will address questions such as:

- How can we ensure that digitizing victim records and connecting them to government or third-party services does not increase the risk of harm for persons whose data is shared, including vulnerable individuals and communities?
- What shared standards or audit mechanisms can be implemented to prevent unauthorized access, data misuse and data breaches and ensure transparency and accountability in the event of such incidents?
- What are the minimum technical and legal standards required to ensure that data stored in Digital Victim Registries meets evidentiary standards for use in justice settings?
- How do we design "trauma-informed" consent mechanisms so that victims can set, amend, or withdraw permissions for data-sharing, through meaningful control in real-time and throughout the data lifecycle?
- Given the costs of maintaining blockchain-based ledgers, are there simpler high-integrity digital audit trails that may be more suited to resource-constrained settings?

5. Creating a safer internet for victims of terrorism

Problem Statement

Digital platforms can contribute to further trauma to victims and survivors of terrorism through the misuse or manipulation of images of victims, algorithmic amplification and feedback loops and the persistent circulation of graphic imagery. From deepfakes used to discredit victims to the unauthorized memorialization of private profiles, the digital environment can exacerbate psychological distress long after the physical event. Creating a safer internet for victims of terrorism requires efforts beyond the moderation or removal of “illegal”, “terrorist” or “violent extremist” content. It calls for a comprehensive approach to addressing online harms that is firmly grounded in international human rights norms and standards, protects the rights and dignity of victims of terrorism and at the same time safeguards freedom of expression.

Beyond Content Removal

As discussed in the Gap Analysis of Digital Tools to Support Victims of Terrorism, technical and institutional frameworks are evolving beyond narrow content takedown approaches to address the complex ecosystem of modern disinformation and harmful online content. Crisis protocols have matured through initiatives such as the Global Internet Forum to Counter Terrorism (GIFCT), which utilizes a hash-sharing database to identify and remove terrorist and violent extremist content across thirty-three platforms. To counter "synthetic" harms, tools like SynthID and C2PA provide digital authenticity markers crucial for debunking deepfakes, as seen after the 2025 Bondi Beach attack. Finally, violence prevention services from organizations like Moonshot and Parents for Peace are now being signposted directly to users consuming violent content, with a view to providing targeted, preventative and support-oriented interventions.

Core Questions for the Working Group

With a view to establishing a roadmap for a safer internet for victims of terrorism, this working group will address questions such as:

- How can platforms implement priority reporting channels for verified victims of terrorism to ensure that their reports are escalated beyond automated systems and are reviewed promptly by human moderators trained in trauma-informed care?
- What technical standards are required to neutralize the viral "trending" of graphic footage and increase hash-detection sensitivity during high-risk windows like attack anniversaries?
- How do we develop trauma-informed approaches for content that is legal but may nonetheless cause harm, that recognize re-traumatization and secondary trauma, and work towards mitigating harms in a manner consistent with international human rights norms and standards?
- What are the design requirements for robust keyword disruption and "conscious viewing" friction, such as pop-up warnings, that allow victims and survivors to curate their own digital safety?
- How can we establish "Golden Hour" crisis response to coordinate verified facts and "safe to share” material to reduce the impact of harmful or misleading narratives immediately following an event?