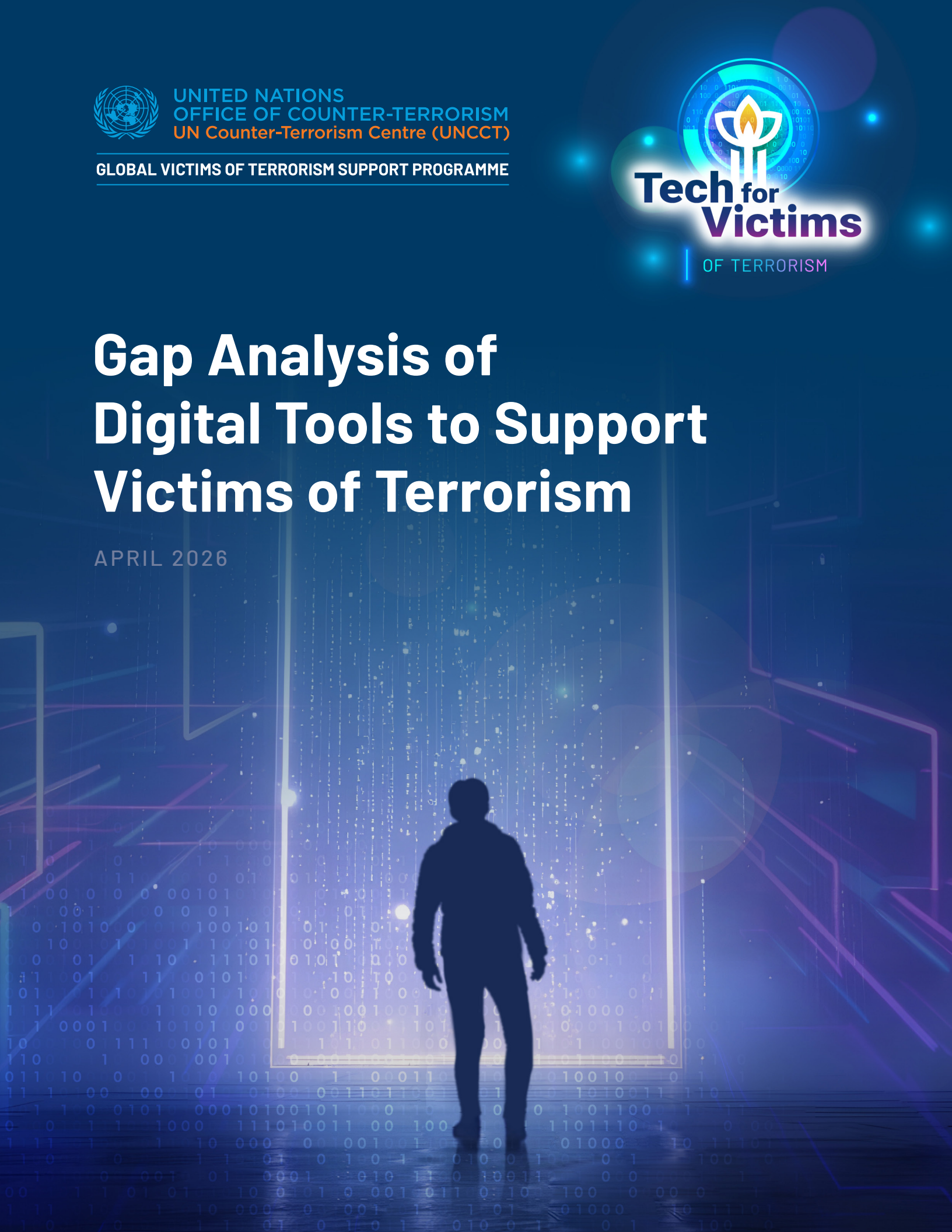
UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)

GLOBAL VICTIMS OF TERRORISM SUPPORT PROGRAMME

Tech for Victims
OF TERRORISM

Gap Analysis of Digital Tools to Support Victims of Terrorism

APRIL 2026



Disclaimer

The opinions, findings, conclusions, and recommendations expressed herein do not necessarily reflect the views of the United Nations or its officials or any other national, regional, or global entities involved. The designations employed and material presented in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area of its authorities, or concerning the delimitation of its frontiers or boundaries. All queries on rights and licences, including subsidiary rights, should be addressed to: United Nations Office of Counter-Terrorism United Nations Headquarters New York, NY 10017, USA

Acknowledgements

This report was prepared by the United Nations Office of Counter-Terrorism (UNOCT) through the Global Victims of Terrorism Support Programme with the support of a consultant Emily Knowles. Gratitude is extended to the peer review provided by Adriana Banozic, Amy Nitza, Arnaud Kurze, Caroline O'Hare, Einat Halevy Levin, Imrana Buba, Jibu Elias, Michael O'Connell, Sallie Lynch, Salvador Dura-Bernal, and Zahida Virani, as well as the contributions of the Victims of Terrorism Associations Network (VoTAN). UNOCT also expresses its appreciation to the survey respondents and experts who participated in bilateral consultations, generously sharing their knowledge and time to shape and strengthen this report.

This report was made possible thanks to the financial support of the German Federal Foreign Office.

United Nations Office of Counter-Terrorism
United Nations
405 East 42nd Street
New York, NY 10017

uncct@un.org

@un_oct | #uncct

www.un.org/uncct

Contents

Abbreviations and acronyms

AI	Artificial Intelligence
BITS	Belgian Incident Tracking System
DSA	Digital Services Act, EU
DISHA	Data Insights for Social and Humanitarian Action, UN
DPI	Digital Public Infrastructure
EBT	Evidence-Based-Therapy
EEG	Electroencephalogram
EU	European Union
FBI	Federal Bureau of Investigation, US
GCAIMH	Global Center for AI in Mental Health
GIFCT	Global Internet Forum to Counter Terrorism
GPT	Generative Pre-trained Transformer
HDX	Humanitarian Data Exchange
IACP	International Association of Chiefs of Police
IASC	Inter-Agency Standing Committee, UN
IDMC	Internal Displacement Monitoring Centre
INTERPOL	The International Criminal Police Organization
INVICTM	International Network Supporting Victims of Terrorism and Mass Violence
IOM	International Organization for Migration
IRC	International Rescue Committee
IRF	Incident Response Framework
ISD	Institute for Strategic Dialogue
LLM	Large Language Model
NCVC	National Center for Victims of Crime
NMVC	National Mass Violence Center
MHPSS	Mental Health and Psychosocial Support
MIPP	Major Incident Public Portal, UK
NGO	Non-governmental organization
OCHA	United Nations Office for the Coordination of Humanitarian Affairs
OVS	Office of Victim Services
PFA	Psychological First Aid
PTSD	Post-Traumatic Stress Disorder
RAN	Radicalisation Awareness Network, EU
SAMHSA	Substance Abuse and Mental Health Services Administration, US
TTX	Tabletop Exercise
UNCCT	United Nations Counter-Terrorism Centre
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNHCR	United Nations High Commissioner for Refugees
UNOCT	United Nations Office of Counter-Terrorism
VoTAN	Victims of Terrorism Associations Network
VR	Virtual Reality

Foreword

Terrorism has profound and lasting impacts on victims, and their needs must remain at the center of our collective efforts. The United Nations Office of Counter-Terrorism (UNOCT) remains firmly committed to supporting Member States and partners in strengthening assistance to victims in ways that uphold their rights, dignity, and agency.

When applied responsibly, digital technologies offer new opportunities to enhance how Member States, international organizations, and civil society deliver support. These technologies can help expand access to essential services, strengthen coordination across support services and providers, and ensure that assistance reaches victims and survivors of terrorism wherever they are, including in underserved and high-need contexts.

From AI-driven mental health tools to digital service referral systems, these innovations can help address longstanding gaps in victim support. At the same time, they must be anchored in human rights, robust data protection safeguards, and victim-centered design, so that the assistance they provide is safe, inclusive, and dignified.

This Gap Analysis of Digital Tools to Support Victims of Terrorism marks an important step forward. It builds on UNOCT's broader efforts to leverage new technologies to prevent and counter terrorism, while placing emphasis on supporting those most affected. The report identifies opportunities for digital tools to enhance support to victims and survivors of terrorism across four key areas: providing services, supporting justice and accountability, protecting against revictimization, and fostering peer support and victim empowerment.

Importantly, the analysis underscores that victims, survivors and affected communities must be active participants in shaping the solutions designed to support them. Digital tools are most effective when they are co-created with victims and grounded in lived experience, ensuring that they respond to real needs and diverse contexts.

Significant work remains. Cross-sectoral expertise and partnerships are essential to bring safe and effective digital tools to victims of terrorism, first responders, and service providers. At the same time, we must continue to bridge digital divides, so that technological advances narrow, rather than deepen, existing inequalities.

With the support of the German Federal Foreign Office, UNOCT will continue this work through dedicated initiatives to refine victim-centered design principles for digital and online spaces and to develop a Toolkit for Technology-Enabled Support to Victims. We urge all stakeholders – across governments, the private sector, academia, and civil society – to join in translating these findings into practice.

I especially wish to thank the victims and all other experts whose insights have shaped this analysis. Looking ahead, UNOCT, through its United Nations Counter-Terrorism Centre (UNCCT), will continue to prioritize the needs of victims of terrorism. In an era of rapid digital change, our mission remains unchanged: to stand in solidarity with victims of terrorism, to strengthen their voices, to improve practical resources available to them, and to support the capacity of others to uphold the rights of victims and meet their needs.

Alexandre Zouev
Acting Under-Secretary-General
of the United Nations Office
of Counter-Terrorism

Executive Summary

New and emerging technologies are among the most profound drivers of global change. When used responsibly, they offer the potential to enhance how Member States, international organizations, and civil society provide assistance to victims and survivors of terrorism.

From AI-enhanced training for first responders to digital platforms that connect survivors to essential care, these tools provide new opportunities to strengthen victim support systems, improve coordination and bridge longstanding access gaps across the globe, including in underserved contexts or surge situations following a terrorist attack.

Harnessing technology for the public good requires global cooperation and a clear alignment with human rights principles. As the multi-stakeholder United Nations High-level Advisory Body on Artificial Intelligence noted in its final report,[1] pooling scientific knowledge is most efficient at the global level, enabling joint investment and public interest collaboration across otherwise fragmented and duplicative efforts. The Pact for the Future[2] and the Global Digital Compact,[3] adopted by Member States in 2024, further reinforce the global commitment to closing digital divides and ensuring that technology is used to promote the rights and needs of all humanity, providing a vital foundation for leveraging digital tools to enhance support for victims and survivors of terrorism.

1 https://www.un.org/ai-advisory-body
2 https://www.un.org/en/summit-of-the-future/pact-for-the-future
3 https://www.un.org/digital-emerging-technologies/global-digital-compact

The United Nations Global Counter-Terrorism Strategy[4] and its subsequent reviews call upon Member States to ensure that the physical, medical and psychosocial needs of victims are met, and to develop comprehensive assistance covering immediate, short-term and long-term needs. The Strategy further emphasizes the importance of engaging with a wide range of stakeholders, including academia, the private sector and civil society, in advancing comprehensive and effective responses to terrorism, including support to its victims and survivors and in leveraging digital technologies in a safe and rights-respecting manner.

Against this backdrop, this "Gap Analysis of Digital Tools to Support Victims of Terrorism", published by the United Nations Office of Counter-Terrorism (UNOCT), identifies the most critical gaps in victims support and survivor care that can be addressed through digital innovation. It shows that digital tools can significantly strengthen the accessibility, timeliness, and reach of support for victims and survivors of terrorism, while helping to ensure that assistance is delivered in a safe, inclusive, and dignified manner that respects the agency and rights of victims and survivors.

The Gap Analysis also provides recommendations for victim-centered design of digital support tools, including in low-connectivity and resource-constrained settings. The findings are rooted in extensive research, including interviews with the private sector and academia, a global mapping of digital tools, and a peer-review process involving experts and members of UNOCT's Victims of Terrorism Associations Network (VoTAN), which brings together the critical lived experience of over 120 victims of terrorism and victims' associations from 40 countries worldwide.

The report represents the first deliverable of a new "Tech for Victims of Terrorism" initiative, implemented by UNOCT through its United Nations Counter-Terrorism Centre (UNCCT) Global Victims of Terrorism Support Programme, with the support of the German Federal Foreign Office. The project seeks to align new technologies with the needs of victims and survivors of terrorism to establish a clear path for safe, responsible, and victim-centric digital innovation.

4 https://docs.un.org/en/A/RES/77/298

Introduction

Every victim of terrorism has a unique journey, yet many share fundamental needs. The Global Victims of Terrorism Support Programme was established in 2018 to stand in solidarity with victims of terrorism, strengthen victims' voices and their role in preventing and countering violent extremism conducive to terrorism, establish stronger mechanisms to provide practical resources to victims and survivors, and strengthen the capacity of Member States and civil society organizations to assist and support victims of terrorism in protecting and promoting their rights and needs.

This includes developing tools that respond to the priority needs of victims and advance the international victims of terrorism agenda, in close collaboration with the Victims of Terrorism Associations Network (VoTAN),[5] which was launched in April 2025 and comprises over 120 victims of terrorism and victims' associations from over 40 countries around the world.

VOTAN
Victims of Terrorism Associations Network

Our work identifies four core priorities that reflect the evolving nature of terrorism and its long-term impact on individuals and communities, informed by the outcomes of the 2022 Global Congress on Victims of Terrorism,[6] the 2024 International Conference on Victims of Terrorism in Spain,[7] and direct consultations with the Victims of Terrorism Associations Network (VoTAN)[8]:

The Four Core Priorities

1. **Comprehensive, Long-Term Support**
2. **Justice & Recognition**
3. **Protection from Re-Victimization**
4. **Agency & Empowerment**

5 https://www.un.org/counterterrorism/en/events/launch-victims-terrorism-associations-network-votan
6 https://www.un.org/counterterrorism/sites/default/files/global_congress_report_september_2022.pdf
7 https://www.un.org/counterterrorism/sites/default/files/2024_vot_international_conference_report.pdf
8 https://www.un.org/counterterrorism/sites/default/files/2026-03/victims_of_terrorism_association_network_-_contribution_to_sg_report_on_activities_of_the_un_in_implementing_the_un_gcts_2025.pdf

1 Comprehensive, Long-Term Support

Beyond immediate crisis care, victims require sustained access to healthcare, legal aid, and psychosocial support. In many regions, recovery also depends on securing housing, education, and livelihood opportunities, especially where social safety nets are weak.

2 Justice & Recognition

Victims often face significant barriers to legal redress. These are compounded by the lack of a universal definition of terrorism, while domestic definitions can be vague or overly broad, sometimes leading to outcomes that deny survivors the formal recognition and support they deserve.

3 Protection from Re-Victimization

In the digital age, trauma is often compounded online. Victims are increasingly vulnerable to secondary trauma through the misuse of technology, including AI-generated deepfakes, disinformation, and extremist propaganda. Building "digital resilience" is now as critical as protecting against offline forms of retraumatization.

4 Agency & Empowerment

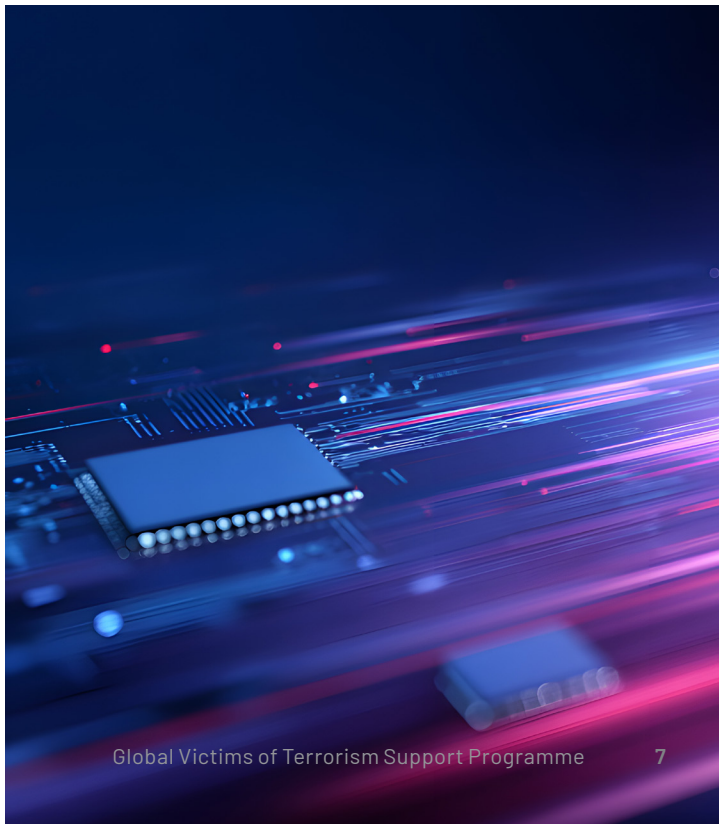
Victims are not merely passive recipients of aid; they are "agents of change" and experts by lived experience. Meaningful engagement means integrating diverse voices, including women and youth, into the design of policies and the digital tools intended to support them.

This report maps existing digital tools that could be adapted for victim support while identifying promising opportunities for future development. However, it is worth noting from the outset that digital tools are not a substitute for well-resourced, in-person care. Where face-to-face support is available, technology should augment, not replace, human interaction. Nonetheless, in many contexts, particularly in least developed countries or during the "surge" following an attack, digital solutions can fill critical gaps in service delivery.

Designing for victims of terrorism also requires a commitment to safety-by-design. The use of Artificial Intelligence (AI) in this space introduces serious concerns regarding data sensitivity, the accuracy of algorithmic inferences, and the potential for irreversible harm. Robust human rights safeguards and oversight mechanisms are non-negotiable to ensure these systems are trustworthy and secure.

In addition, accessibility is a core requirement, not a peripheral concern. Some victims suffer physical or cognitive impairments that require specific visual, auditory, or motor adaptations. Furthermore, tools must be functional in low-connectivity environments and able to support communities, cultural contexts, and languages often underrepresented in the training data of Large Language Models (LLMs).

Finally, we acknowledge the extraordinary speed of digital change. The gap between the capabilities of eighteen months ago and today is vast, particularly regarding generative AI. While this offers new opportunities for multilingual and accessible support for victims of terrorism, it also increases the threats of disinformation and amplifies other sources of potential harm. As such, this analysis represents a snapshot in time that will require frequent review to remain relevant in an ever-shifting digital landscape.



Methodology

The research behind this report was gathered through an in-depth literature review, an online survey, semi-structured interviews with subject matter experts, and an iterative peer review process with representatives from the Victims of Terrorism Associations Network (VoTAN), academia, and industry. Given the pace of technological change and relatively small sample sizes, the resulting gap analysis is not intended to be an exhaustive list of all the tools and platforms currently available or under development. Instead, this analysis serves as a foundational "mapping" to understand the potential of digital and emerging tools across the areas of priority need identified by victims of terrorism.

Each step is outlined below:

1 Literature review

A great deal of existing research and thinking has already been done around several of the distinct areas in this report, including on supporting the mental health and psychosocial (MHPSS) needs of individuals and populations affected by trauma, making AI tools accessible across multiple linguistic and cultural contexts, leveraging tools like blockchain in the justice sector, tackling a rise in mis-/disinformation on the internet, and the promised future connectivity of government digital services provided by Digital Public Infrastructure (DPI) research. A series of targeted keyword searches, supplemented by a review of the documents and articles collated and shared during the peer review process, provided the foundation for the findings presented in this final report.

2 Online survey

UNOCT conducted a targeted online survey seeking submissions of promising digital tools with the potential to support victims of terrorism and first responders. The survey specifically welcomed tools originally designed for other humanitarian, development, or peacebuilding contexts (such as crisis and disaster response, conflict, and criminal justice) where the functionality could be adapted. A total of twenty-five submissions were received covering innovative approaches for accessing health or legal services, psychosocial support, trauma-informed training, service referral, victim registration, documentation of harms, media monitoring, and compensation payment systems. Innovations using AI or other emerging technologies were prevalent, and submissions were received from governments, non-governmental organizations (NGOs), private sector, academia, frontier labs, and international organizations.

3 Semi-structured interviews

UNOCT conducted semi-structured interviews with twenty-one stakeholders from the private sector, academia, civil society, and across the United Nations system to explore existing uses of new and emerging technologies. Participants were identified using a snowball methodology whereby many respondents to the initial survey or authors of research identified in the literature review agreed to speak to the author in more depth about their work and then helped to identify others within their network with interesting perspectives or experience to add to these topics.

4 Peer review

A preliminary draft of this report was reviewed by a twelve-person Peer Review Committee comprising members of the Victims of Terrorism Associations Network (VoTAN) as well as representatives from academia and industry. A series of six drop-in sessions were organized to suit different time zones, and written feedback was also encouraged. This served to strengthen the findings, deepen the treatment of risks, and expand on key points including the addition of important material on building the digital resilience of victims and terrorism-affected communities, integrating victim consultations into existing product development workflows, accessibility-by-design, and building trustworthy AI for use in crisis settings.

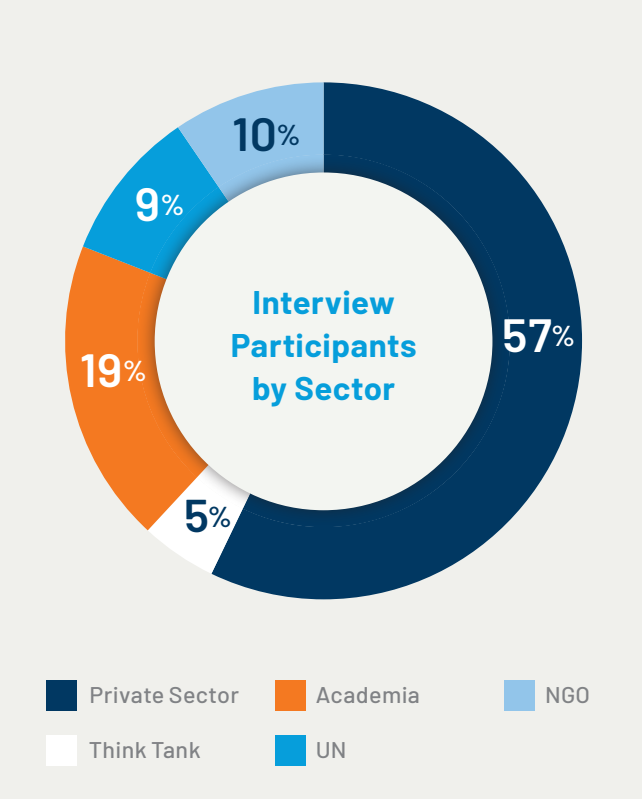


Figure 1: *Interview participants by sector. Private sector includes frontier labs, start-ups, and a range of small to large technology companies.*

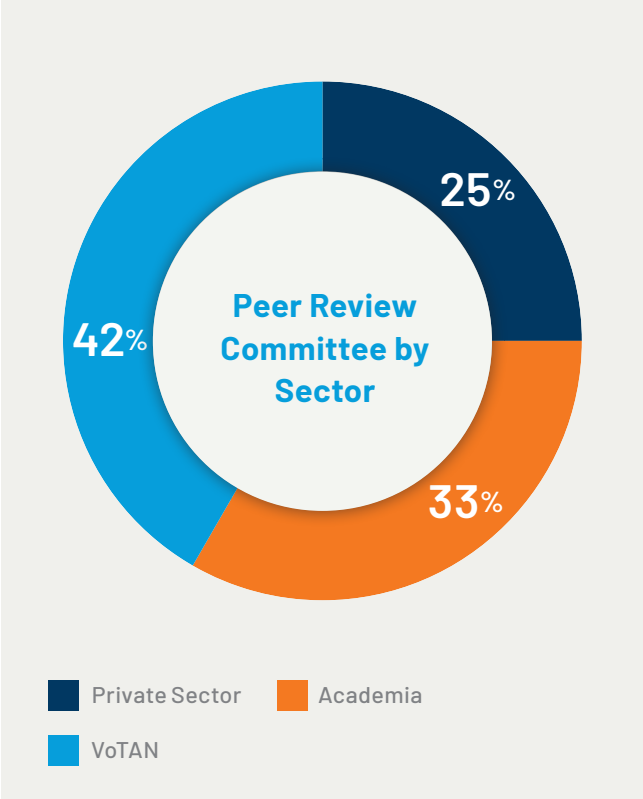


Figure 2: *Members of the peer review committee by sector. Participants contributed a range of in-person and written feedback on a preliminary draft of this report.*

Key Findings

Our analysis finds that digital and emerging technologies have the potential to offer powerful, scalable opportunities to strengthen victim support across all four priority needs identified by victims of terrorism:

1. Providing comprehensive and long-term support services
2. Supporting justice and accountability
3. Protecting against revictimization
4. Supporting victim empowerment and agency

Because victims' needs evolve over time, different tools with different functionalities are applicable at different points in their recovery. Someone in acute crisis needs something very simple, perhaps just a single tap to reach a person. Later, someone engaging with a peer advocacy platform may be ready for much richer functionality.

The four distinct sections and categories of digital support to victims of terrorism presented in this report represent the current state of play of digital tool development in this space, which tends to be siloed between a range of different standalone initiatives, pilots, and research.

Timeline of victim needs and corresponding tools

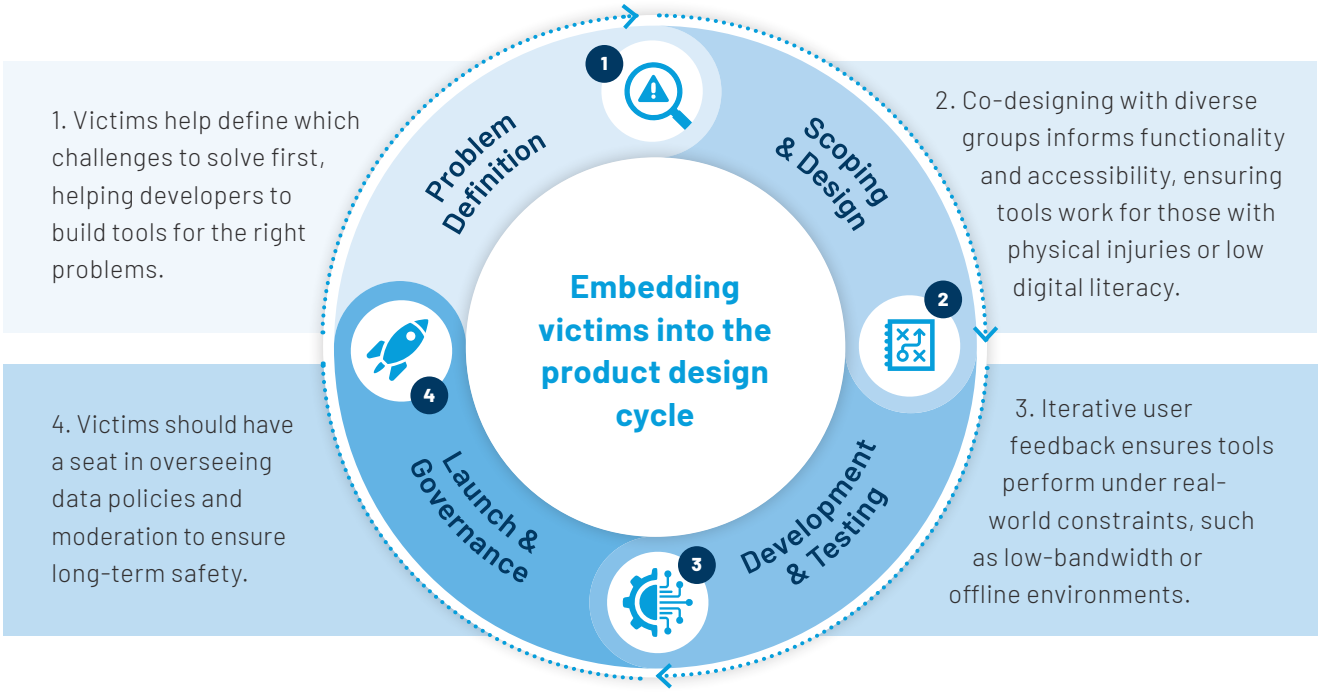
Hours to Days

Digital victim registration, shelter-in-place notification systems, crisis MHPSS (grounding, Psychological First Aid), family notification, immediate financial assistance, or digital payments. Tools used during this surge support must be extremely simple and low friction: the priority is access, not sophistication.

Days to Weeks

One-stop-shop service referral, MHPSS triage and navigation, access to legal aid, connection with victims' associations. Tools used during this services support phase can be slightly more complex but must still work in low-connectivity contexts.

However, in the longer-term, relevant national, regional, and international initiatives could establish an integrated digital victim support infrastructure to connect these areas. Common governance and data guardrails could create a foundation whereby specialized services from AI mental health tools to justice platforms could be seamlessly integrated and surged post-incident, perhaps as a digital corollary to the comprehensive assistance plans for victims of terrorism that Member States are already urged to adopt under the United Nations Global Counter-Terrorism Strategy. Finally, finding appropriate ways to co-design with victims of terrorism and terrorism-affected communities is essential to ensure that tools have a positive social impact, as well as to ensure that they are used and useful to communities. We have suggested some ways to do this in the report, but this is an area that deserves more detailed work and guidance development in the future.



Weeks to Months

Ongoing psychosocial support, peer connection, compensation access, educational opportunities, return to work or school. This early recovery phase is where peer support and learning platforms may become more realistic.

Years

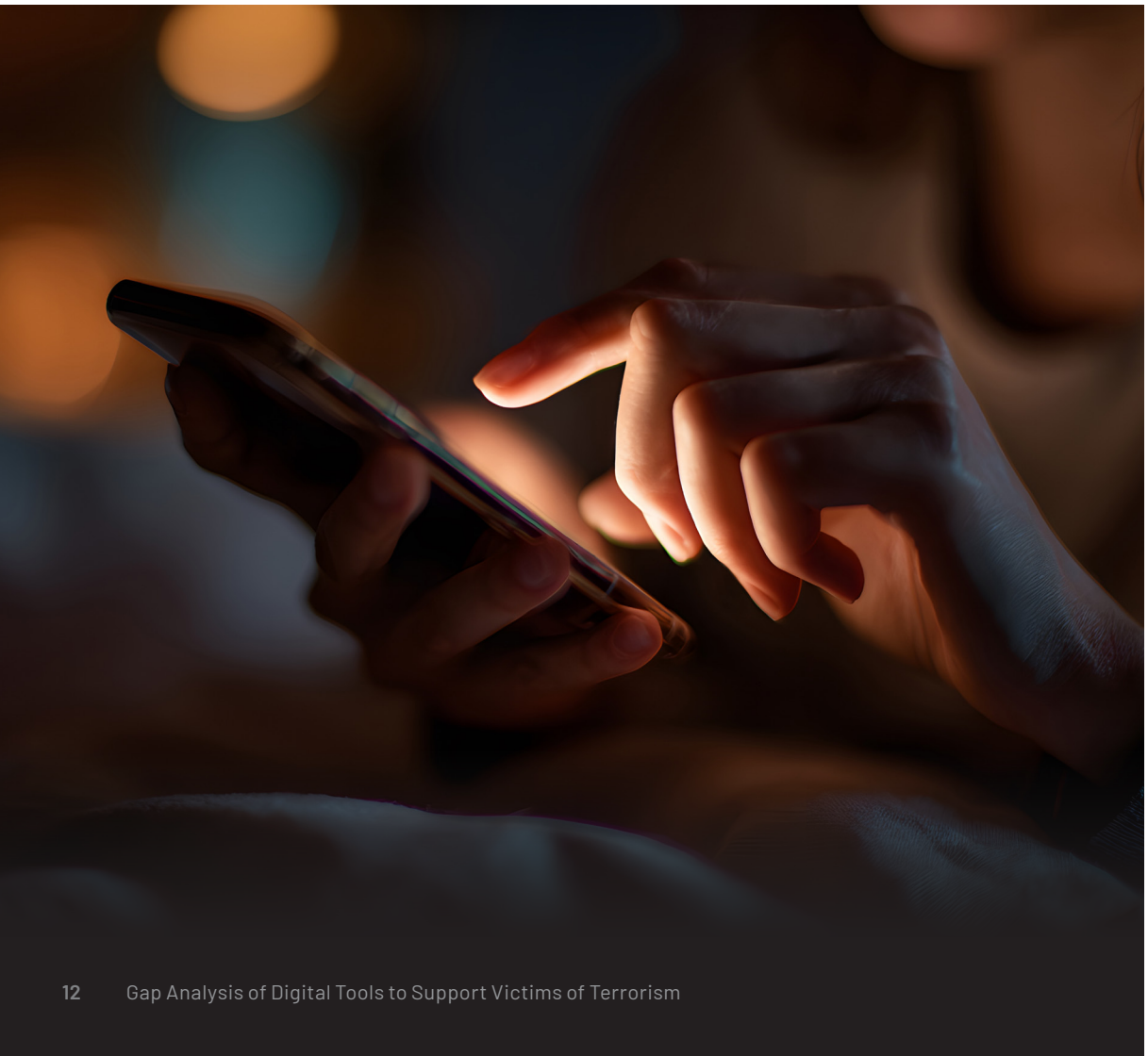
Justice proceedings, commemoration, long-term advocacy, platform-based community. Evidence preservation and cross-border case management tools become more important here, as well as the transition of tools from the early recovery phase into long-term support and care.

While the analysis is geared towards addressing the needs of victims of terrorism specifically, it draws heavily from tools and materials that were developed for other humanitarian, development, or peacebuilding contexts. Its findings may be applicable to designing and developing social impact tools for a broader range of crisis-affected communities.

However, we must recognize that this report is a snapshot of a rapidly shifting field. As AI-generated deepfakes and automated disinformation become more sophisticated, the retraumatization risks for victims of terrorism grow.

Conversely, the potential for multilingual, highly accessible support is also expanding. Constant re-evaluation is required to ensure that the gap between technological developments and victims' needs does not widen.

Ultimately, we hope this analysis inspires the public-private partnerships and social entrepreneurship needed to turn these digital possibilities into a global reality for individuals in their hour of need.



Report structure

The report is divided into four thematic sections that respond to the four priority needs identified by victims of terrorism:

1. Providing comprehensive and long-term support services
2. Supporting justice and accountability
3. Protecting against revictimization
4. Supporting victim empowerment and agency

The four priorities are presented as discrete categories, but in the future digital victim support services could become deeply interconnected. For example, a digital victim registry (Priority 1) could serve as the platform through which survivors access peer-to-peer support (Priority 4), are referred to mental health services (Priority 1), participate in community moderation groups to remove traumatizing content from social media (Priority 3), or manage their consent for judicial proceedings (Priority 2).

The report then covers considerations for victim-centered tool design and common risks and limitations that need to be taken into account when designing and developing digital tools for victims, including human rights and gender considerations, trust and safety considerations, accessibility and sustainability considerations, and additional considerations when developing for low-connectivity and low-resource settings.

The report also provides vignettes based on the existing state of play or expected near-term capabilities of a range of digital tools and solutions that have the potential to meaningfully improve the lives and experiences of victims of terrorism, including in low-connectivity and low-literacy settings.

1. Providing comprehensive and long-term support services

This section is split into two chapters, the first on digital tools for mental health and psychosocial support, and the second on ways to use new and emerging technologies to enhance digital victim registration and service referral following an incident. It profiles existing and emerging tools designed to be victim-facing (for example mental health apps), clinician-augmenting (for example tools to support a wide range of community workers, psychological first aid providers, and specialist clinicians), government-focused (for example digitizing post-incident victim registries), and service provider-supporting (for example signposting victims towards available support services whether provided by governments or NGOs).

2. Supporting justice and accountability

This section covers an emerging area of research into the use of permissioned ledgers, smart contracts, homomorphic encryption, and digital public infrastructure in the judicial system. It covers the use of blockchain technology to log evidence, manage variegated access to victim testimony, facilitate cross-border information exchange between justice systems, and put victims in charge of their own data and how it can be accessed, used, and stored.

3. Protecting against revictimization

This section covers ways to leverage new and emerging technologies to reduce the risk that victims are further traumatized post-incident. It is split into two chapters, the first on improving trauma-informed and victim-centered interviewing and incident management by first responders and government agencies, and the second on tools to reduce the risk of traumatization through the circulation of attack footage, mis-/disinformation, and identifying information about victims and their families in traditional and social media.

4. Supporting victim empowerment and agency

This section covers ways to use digital tools and platforms to empower victims of terrorism and restore their agency following an attack. It is split into two chapters, the first on the use of digital platforms to increase peer-to-peer support and learning following an incident, and the second on tools to build the digital resilience of victims and their communities.

PRIORITY 1

Providing Comprehensive & Long-Term Support Services

Digital tools for mental health and psychosocial support

Digital mental health and psychosocial support (MHPSS) has evolved into a diverse ecosystem capable of augmenting traditional care and filling gaps where sustained, in-person support is not available. These tools offer faster access, wider reach, and a path to more consistent quality services that could be surged following a crisis and then maintained over the medium to long term. Existing tools tend to serve a few different functions: supporting victims directly, assisting non-specialist providers (such as first responders, family, and community members), and supporting clinicians. They can also support the mental health needs of care providers themselves.

It is worth recognizing at the outset of this section that the integration of AI into mental health must be approached with caution. The risk profile of a tool changes significantly based on its "closeness" to the victim and its level of human supervision.

For example, tools drawing from a vetted corpus of medical research are significantly safer than those using generative AI for conversational therapy. Frequent interaction with unsupervised AI chatbots has shown potential for negative mental health effects, particularly among youth and vulnerable populations.[9] For high-stakes emotional support in crisis settings, human-in-the-loop validation remains essential to prevent AI "hallucinations" or incorrect advice that could harm victims. In addition, given the sensitivity of MHPSS data, technical features must ensure robust anonymization and secure storage to build user trust and comply with international data protection standards. It is also worth bearing in mind that not all tools designed for MHPSS are adapted for victims of terrorism who may be suffering from severe trauma, including Post-Traumatic Stress Disorder (PTSD).

9 https://med.stanford.edu/news/insights/2025/08/ai-chatbots-kids-teens-artificial-intelligence.html, https://www.theguardian.com/technology/2026/jan/08/google-character-ai-settlement-teen-suicide

What could good look like?

For a future victim with access to some in-person clinical support

It is three days since the attack. A victim opens a trauma-informed app that offers three paths: breathe, sleep, or talk to someone. On selecting 'breathe,' a gentle coach voices a two-minute grounding, then suggests a short body-scan meditation. The app pairs with the victim's smartwatch to track heart rate, and when their pulse spikes during the scan, it automatically slows the breathing pace and switches to haptic cues. A journal prompt appears with a large microphone: "Say what feels hardest right now." The transcript stays on-device by default. With a clear toggle, the victim can share a daily summary of heart-rate trends, sleep duration, and selected notes with their assigned clinician. Most functionality is available even offline, live support is always one tap away, and the app reminds the victim they can turn off sharing information with their assigned clinician at any time.

For a future carer in a low-connectivity setting

A community MHPSS worker is about to head out to conduct a round of check-ins with victims of a recent terrorist attack. Before leaving, they use Wi-Fi to download an offline "visit pack": short audio clips, pictogram guides, and a lightweight chatbot tuned for the local dialect. When they sit down with a victim, they launch the offline pack. They ask the chatbot for advice when a victim reports they have a tight chest and can't sleep. The bot retrieves a pre-cached answer from vetted medical and psychosocial sources and reads out a two-step plan in the local dialect, with pictured breathing and sleep-hygiene tips that display without data. The carer plays a one-minute audio explaining grounding and shows an image sequence for paced breathing. They practice the breathing technique together. Feeling unsure about a question about flashbacks, the carer records a short note; the app stores it locally and marks it for supervisor review when connectivity returns. At day's end, the community worker's visit reports and flagged notes auto-sync, and the next day's notes are updated to reflect more detailed advice about the symptoms they report encountering often.

What's currently out there?

- **Mindfulness apps:** For people with PTSD, mindfulness practices have proven helpful for stress regulation, sleep, emotion regulation, and distress tolerance. A range of MHPSS and mindfulness apps are currently on the market, with top entries on the Apple app store including Headspace and Calm.[10] Electroencephalogram (EEG) neurofeedback tools such as the Muse headband offer brain signal processing and real-time feedback that can be used for relaxation, meditation, sleep, as well as PTSD.[11] Real-world observational studies of commercial app users often show perceived stress reductions associated with engagement, especially for frequent users.[12] However, randomized trials of tools aimed at PTSD sufferers specifically generally find small, short-term improvements in depression and anxiety.[13] Standalone mindfulness apps are not well-established as PTSD treatments in the way in-person trauma-focused psychotherapies are,[14] although they remain grounded in stronger research than more experimental uses of digital tools in this space.

- **Remote MHPSS entry points and hotlines:** Services such as the International Organization for Migration (IOM)'s Emotional Support Hotline for Ukraine allow callers to receive psychological first aid (PFA) and referral to tailored services, including consultations with hotline psychologists or referrals to in-person services in their communities when available.[15] Hala Systems' Respond tool was deployed in Syria to facilitate rapid, secure health referrals in conflict-affected environments, addressing the need for real-time coordination among field responders, medical providers, and humanitarian actors.[16] National platforms like Singapore's Mindline provide app-based prevention, self-help, and MHPSS triage for broad populations, with escalation into in-person care where necessary,[17] while PureHealth, one of the largest healthcare groups in the Middle East, has launched virtual mental health services across the United Arab Emirates through the Pura app, which provides virtual therapy and emotional resilience tools and can connect users to licensed clinical support and in-person services if necessary.[18]

- **Clinician-facing tools:** Organizations like the Global Center for AI in Mental Health (GCAIMH) are partnering with the private sector to build and pilot tools to support MHPSS clinicians and first responders. For example, a collaboration with Google focuses on assisting clinicians to deliver Evidence-Based-Therapy (EBT) by using voice agents, AI transcription and LLMs to provide real-time recommendations to clinicians based on analysis and evaluation of a patient's cognitive and emotional state. In between sessions, the tool is designed to offer advice to clinicians to improve their overall approach to EBT through an analysis of key therapeutic moments, which feeds reports on progress indicators and areas for improvement, as well as specific follow-up recommendations for individual cases.[19] Startups like Jimini provide 24/7 AI behavioral health assistants to support patients between sessions with their MHPSS provider and help clinicians to track patient progress.[20]

- **AI support to non-specialist MHPSS providers:** GCAIMH are also working on a joint initiative with IBM developing a digital tool to support non-specialist Psychological First Aid (PFA) providers in disaster settings, drawing on a corpus of expert PFA research to provide real-time guidance and practical information to providers and first

10 https://apps.apple.com/us/story/id1599762531
11 https://choosemuse.com/pages/muse-research
12 https://pmc.ncbi.nlm.nih.gov/articles/PMC10986332/
13 https://pmc.ncbi.nlm.nih.gov/articles/PMC10215014/, https://doi.org/10.1016/j.jad.2020.09.134, https://link.springer.com/article/10.1007/s12671-018-1050-9 https://pmc.ncbi.nlm.nih.gov/articles/PMC10215014/, https://doi.org/10.1016/j.jad.2020.09.134, https://link.springer.com/article/10.1007/s12671-018-1050-9, https://journals.sagepub.com/doi/abs/10.1177/1524838018781103
14 https://www.ncbi.nlm.nih.gov/books/NBK606175/
15 https://ukraine.iom.int/sites/g/files/tmzbdl1861/files/documents/2025-05/iom_ukraine_mentalhealthandpyschosocialsupportoverview_digital-3.pdf
16 https://www.halasystems.com/
17 https://mindline.sg/
18 https://www.khaleejtimes.com/lifestyle/mental-health/uae-mental-health-services-ai-app, https://purehealth.ae/purehealth-has-launched-sakina-the-regions-largest-mental-health-platform/
19 https://www.gcaimh.org/research-initiatives
20 https://jiminihealth.com/

responders as they work with affected individuals.[21] Organizations like The After Collective have developed an AI chatbot-based recovery coach that provides text-based disaster emotional support to users and PFA resources for first responders.[22] Acknowledging the important role of community workers and mental health focal points in low-resource and conflict-affected settings, Google, McKinsey Health Institute, and Grand Challenges Canada, recently collaborated on a Mental Health and AI Field Guide that covers use cases including provider-client matching, AI training, severity triage, and real-time AI companions for non-specialist carers.[23]

- **Digital therapeutics:** The National Mass Violence Center (NMVC) in the United States hosts the Transcend mobile app, which provides self-help guidance to victims following direct or indirect exposure to mass violence incidents. It provides information about common reactions to high-stress events and guides users through strategies to reduce the risk of stress-related behavioral health problems and promote recovery. It can also connect users through to victim and survivor services, and other MHPSS resources.[24] Platforms like MEMOTEXT help organizations build digital engagement and therapeutics tools that can be integrated with wearables and smart assistants, secure chatbots, machine learning analytics, and voice assistants.[25] This has been used to develop tools such as App4Independence (A4i), a mobile digital health intervention for individuals living with schizophrenia-spectrum illnesses that provides daily wellness check-ins, appointment reminders, peer support and a provider dashboard for collaborative care planning.[26]

Potential benefits for victims of terrorism

- **Faster first contact and triage:** Information services and hotlines reduce time-to-referral, critical for reducing distress and surging support to large numbers of victims simultaneously.
- **Consistency and quality of care:** Structured scripts, decision support, and PFA assistive tools can raise the baseline for non-specialist responders and community MHPSS workers, improving both the effectiveness of care and enabling non-specialist responders to take on PFA more confidently, especially with supervision and post-session review by qualified practitioners.
- **Reach at scale:** Online and messaging-first approaches extend supportive contact to those who will not or cannot attend clinics, while normalizing help-seeking and reducing isolation.
- **Safer navigation:** Virtual casework and integrated referral systems improve "right first time" matching between clinicians and those who require care, reducing retraumatization from repeated disclosures to different service providers while searching for adequate support.
- **Adaptability to low-connectivity settings:** Messaging channels, voice hotlines, and offline-capable content packages can function where bandwidth is scarce and literacy is low, providing support for non-specialist and community workers in some of the world's most difficult settings, and opening up MHPSS support to victims who may otherwise not receive this care.
- **Accessibility-by-design:** Voice- and text-based interactions are both currently being developed in the MHPSS space, giving users greater options as to how they choose to interact with tools.

21 https://www.gcaimh.org/research-initiatives
22 https://www.theaftercollective.org/
23 https://www.tasksharing.ai/
24 https://nmvvrc.org/survivors/transcend-nmvc/
25 https://www.memotext.com/about-us/
26 https://www.memotext.com/?marketplace=a4i

Gaps that remain

- **Equitable access, languages, and cultural fit:** Many deployments are still in pilot and have limited language coverage or multilingual abilities. In addition to the translation of materials, literacy and cultural adaptation require development and funding to cover different cultural cues and language around trauma and grief, which is likely to require dedicated work with communities to develop more granular understandings of how MHPSS topics are discussed, including gendered perspectives and potential bias and discrimination.
- **Workforce enablement:** Less experienced clinicians and MHPSS service providers could benefit from augmenting their training with digital tools that allow them to recall and practice their skills. However, the utility of these tools will always be constrained by the number of PFA providers and community MHPSS workers that already exist or can be trained and deployed following a crisis, and tools are designed to complement, not to replace, in-person training.
- **Trust-by-design:** Trust is the foundation of the relationship between a victim and a digital tool. In MHPSS use cases, building this trust requires more than just a privacy policy; it requires transparent, trauma-informed communication about what the tool can and cannot do. This includes clear "human-in-the-loop" hand-offs when a user is in crisis and ensuring that victims engage in the co-design process so that the tool's "voice" feels safe and culturally appropriate rather than clinical or automated.
- **Privacy and security:** Data transmission, particularly when it comes to sensitive patient MHPSS data, and especially in insecure settings or active conflict zones, is risky. Designing apps to withstand malicious attempts to corrupt, access, exfiltrate, or otherwise distort data can be expensive and is not necessarily front of mind for developers, while controlling for inadvertent data disclosures or leaks is also an important consideration. There are no widely agreed standards for data handling, no robust audit mechanisms, and no clear accountability frameworks when tools cause harm, which are important preconditions for any deployment at scale.
- **Risks of harm:** Victim-facing MHPSS tools could trigger or exacerbate existing trauma, for example via unwanted push notifications, algorithmic amplification of trauma-related content, and the emotional burden of maintaining a presence on a platform that constantly surfaces painful memories. In addition, the potential negative psychological effects of sustained interaction with AI chatbots are becoming better known, especially for youth and vulnerable populations. Co-designing tailored tools with victims is one way to reduce this risk, but the creation of safer and more trustworthy tools does not preclude the fact that victims may reach for MHPSS support from general-purpose AI tools and chatbots that may not have trauma-informed safeguards built in. Working with popular platforms to build safe hand-offs of users to more robust and specialized MHPSS tools and services should be considered.
- **Evidence and real-world validation:** Digital mental health tools such as mindfulness apps have a strong research base, but humanitarian-specific psychosocial interventions and those designed specifically for trauma-affected populations are less tested at scale. Practitioners need evidence and implementation toolkits adapted to crisis settings, which requires more pilot studies and established evaluation metrics.

Enhancing digital victim registration and service referral

In the immediate aftermath of a terrorist attack, victims are often overwhelmed by complex bureaucratic requirements at a time of acute vulnerability. Navigating support systems, from proving eligibility to accessing reliable information, frequently falls on the victims and their families. While government liaison officers and victims' associations provide vital aid, the sheer scale and variety of needs following an incident can often exceed existing capacity.

A growing set of digital tools is designed to make that journey simpler. Some focus on rapid intake, such as secure online portals that let victims and witnesses register and share information in a structured way. Others focus on signposting and referral, as digital information services guide people to the right services based on their situation and location. Finally, data triage and analysis tools can help authorities make sense of large volumes of incident reporting by extracting key details and flagging trends to support faster coordination.

Looking ahead, there is significant potential for Member States to integrate digital victim registries into broader Digital Public Infrastructure (DPI).[27] By securely recording identity, consent, and eligibility, these future systems could allow victims to access services seamlessly across different agencies.

However, any digital registration or referral system relies on reliable data and greater data connectivity. For data concerning victims, and especially in politically sensitive or high-risk contexts, robust security protocols and privacy-by-design are not just technical requirements, they are essential safeguards against the malicious or inadvertent disclosure of victim information. To be effective, these systems must prioritize equitable access, ensuring that digital hurdles do not replace physical ones. The Universal DPI Safeguards Framework, launched in 2024, provides a set of practical recommendations to address risks that can arise from DPI implementation.[28]

What could good look like?

For a future government with developed DPI

After a terrorist attack, pre-approved data sharing protocols are activated by the government. Authorized responders from multiple agencies access a common picture, including site layouts, estimated occupancy, and nearby triage capacity through a secure data-exchange platform. Partnerships with mobile networks and providers ensure that anyone within a few miles' radius of the incident receives a shelter in place warning, followed later by directions to the nearest registration points set up at hospitals and police stations to build a digital victims' registry of everyone impacted by the incident. To protect traumatized individuals from lengthy interviews with authorities, Digital ID is used to populate the registry with one tap, and two quick check boxes record preferred language and data sharing preferences. When accessing the record, the registrar only sees what's needed for triage and further service referral. For visitors without local documents, the system issues a temporary credential to ensure equal access. If emergency payments are available, a digital payment arrives at the person's chosen wallet the same day, and secure communications channels can be set up between authorities and victims, bereaved, and wider communities impacted by the incident to provide timely and trusted information updates.

27 https://www.undp.org/digital/digital-public-infrastructure
28 https://www.dpi-safeguards.org/

For a future victim in a high-connectivity environment

Six days after the attack, a victim receives a new notification on their digital victim registry portal. They have been pre-authorized for additional mental health and psychosocial support and have received a QR code that they can show to the list of local and online providers to access care. This QR code serves as proof that they need to go to a local clinic or sign up for digital services, without having to retell their story or show ID. They can filter local and online providers by location, specialization, and availability, and select from a range of in-person and virtual appointments based on their pre-registered language preferences. The app prompts the victim to review and update their data-sharing preferences based on whether they would like to be contacted in the future about other available services, updates on judicial proceedings, or the organization of commemorations or memorials. These preferences can be updated and amended at any time but are set to privacy by default.

What's currently out there?

- **Incident intake portals and registries:** Following a recommendation from the parliamentary inquiry into Belgium's response to a terrorist attack in March 2016, the Belgian Incident Tracking System (BITS) was created as a universal registration system for victims. A bracelet with a unique QR code is given to each victim, and medical posts, hospitals, and centers for uninjured individuals and relatives collect and assign data that can be used to identify victims, assess their state of health, and assist relatives in locating them. Data collected is also used to coordinate medical and psychosocial assistance, including in the longer term.[29] Systems like the UK Major Incident Public Portal (MIPP) support public submissions of evidence and structured registration for victims and witnesses, with onward referral features where enabled.[30] Start-ups like NECX have also worked on victim-led development of service platforms that can link users to available local services and assist service providers in their case management.[31]
- **Information services and signposting:** The National Mass Violence Center (NMVC) in the United States hosts a Virtual Resiliency Center to provide resources to help individuals and communities recover from mass violence and signpost them to local resources and notifications, as well as physical support services, if and when those become available.[32] The United Nations High Commissioner for Refugees (UNHCR) hosts a website to signpost refugees towards relevant information based on their country of origin and the country they are trying to claim asylum in, based on information and communication needs assessments carried out to capture priority needs.[33] The International Rescue Committee (IRC)'s Signpost Initiative provides information services to vulnerable populations, operating as a scalable, rapidly deployable system with tools that can be customized for local contexts. Its AI orchestration platform allows it to coordinate multiple LLMs and functions, working in collaboration with in-person content advisors and information needs assessments conducted with local communities.[34] The UK's National Emergencies Trust is also developing a digital platform in partnership with Siemens, Aviva, and Google to allow anyone in the UK to search and query charitable support on different issues in their area, and hopes to evolve to deliver decision-makers with information about how to leverage existing support in a crisis, and where gaps remain.[35] The live chat and hotline manned by the British charity Victim Support also directs victims of crime in the UK towards available support and services.[36]

29 https://www.healthybelgium.be/en/key-data-in-healthcare/preparedness-and-responses-to-crisis-situations/quality-and-innovation/belgian-incident-tracking-system
30 https://mipp.police.uk/
31 https://necx.org/product/victim-services
32 https://massviolence.help/?utm_source=nmvvrc.org
33 https://help.unhcr.org/
34 https://www.signpost.ngo/
35 https://nationalemergenciestrust.org.uk/annual-report-2024-25/
36 https://www.victimsupport.org.uk/help-and-support/how-we-can-help/

- **Multilingual voice interfaces:** In rural areas of India, residents often lose out on pensions, scholarships, or benefit payments simply because scheme information is hard to navigate and usually written in English. To bridge that gap, collaborators including AI4Bharat (based at IIT Madras), OpenNyAI, and Microsoft introduced Jugalbandi, a generative-AI assistant that villagers can reach through WhatsApp. Community members can send a text or voice question; AI4Bharat's speech recognition transcribes audio, the Indian government's Bhashini translation model converts it to English,[37] and GPT models via Microsoft Azure OpenAI Service retrieve the relevant scheme details from government databases. The reply is translated back and delivered as audio using AI4Bharat text-to-speech. Since its rollout in 2023, the tool has expanded to ten of India's 22 official languages and 171 government programs.[38] The tool's success demonstrates the importance of prior public investment in the Bhashini translation infrastructure, a government-funded layer that provided the underlying language capability.
- **Progress on multicultural AI:** Important efforts are underway to enhance the multilingual and cultural inclusivity of LLMs. For example, Cohere's Aya model is trained on a massively multilingual dataset to support 101 languages, with a specific focus on those that are under-resourced.[39] Google's Amplify Initiative focused on recruiting domain experts across Sub-Saharan Africa to provide deep knowledge on sensitive and salient local issues and create datasets that could test the safety, cultural relevance, and potential harms (e.g., hate speech, misinformation) of AI models in domains like health, finance, and education.[40] To further address and assess cultural biases baked in during the LLM training cycle, researchers have introduced benchmarks designed to evaluate how models navigate diverse global perspectives and cultural nuances (for example WorldView-Bench[41] and CARE[42]), while Cultural Mixture of Adapters (CuMA) aims to address the structural problem of "Mean Collapse," whereby models average out conflicting cultural values included in their training datasets into a generic "global" response.[43]
- **Data triage and analytical tools:** The UN Global Pulse's Data Insights for Social and Humanitarian Action (DISHA) worked with McKinsey and industry partners to highlight unexpected population movement in disaster-stricken regions in near real time using trends derived from telecoms data.[44] Tools like the Internal Displacement Monitoring Centre (IDMC)'s IDETECT[45], Hala Systems' HalaFabric[46], Dataminr's First Alert[47] and Data Friendly Space's GANNET[48] automate the collection and analysis of open-source reporting on internal displacement and other humanitarian incidents, using machine learning and natural language processing to increase data production, extract key information, and classify events in a way that could be useful to track and manage service delivery in the wake of an attack. Clearwater Global and Developmetrics have also been building AI-enabled analytical tools to surface information from humanitarian reporting and improve information synthesis and risk-management.[49]
- **Guidance on the identification and registration of victims of terrorism:** Assembling a comprehensive list of victims following an attack is a challenge. The International Network Supporting Victims of Terrorism and Mass Violence (INVICTM) has published guidance, including on predictable challenges such

37 https://www.unicef.org/digitalimpact/bhashini-ai-making-languages-more-accessible-digital-technology

38 https://news.microsoft.com/source/asia/features/with-help-from-next-generation-ai-indian-villagers-gain-easier-access-to-government-services/, https://www.forbes.com/sites/saibala/2023/05/31/microsoft-has-launched-jugalbandi-a-new-generative-ai-app-for-india/ https://news.microsoft.com/source/asia/features/with-help-from-next-generation-ai-indian-villagers-gain-easier-access-to-government-services/, https://www.forbes.com/sites/saibala/2023/05/31/microsoft-has-launched-jugalbandi-a-new-generative-ai-app-for-india/

39 https://cohere.com/research/aya

40 https://arxiv.org/abs/2504.14105

41 https://arxiv.org/abs/2505.09595

42 https://arxiv.org/html/2504.05154v1

43 https://arxiv.org/abs/2601.04885

44 https://developingtelecoms.com/telecom-business/humanitarian-communications/18281-globe-joins-un-s-disha-pilot-to-provide-data-for-ai-driven-disaster-response.html

45 https://www.internal-displacement.org/monitoring-tools/monitoring-platform/

46 https://www.halasystems.com/

47 https://www.dataminr.com/company/dataminr-for-nonprofits/

48 https://www.datafriendlyspace.org/our-work/gannet

49 https://www.clearwater-global.com/services, https://www.developmetrics.com/, https://www.clearwater-global.com/services, https://www.developmetrics.com/

as providing immediate and multilingual information on where and how people's loved ones are following an attack, reaching those who are not registered by attending medical services or do not self-register following an incident, or duplications or errors in registration.[50]

- **Integrated digital victim services:** Although currently in its preliminary stages, Member State-level discussions over Digital Public Infrastructure (DPI) point to the potential development of digital victim registries that could be linked to other DPI concepts such as Digital ID and Data Exchange. Digital victim registries could interoperate with other referral directories and case systems to help provide joined-up services from different government departments and charitable organizations, while role-based access and consent could be designed so that victims retain the rights over how their data is stored, how it is used, and who has access to it. Once available, these registries could also be used to support justice and accountability efforts so that victims registered for some services (for example MHPSS) can also access the relevant justice or compensation modules through the same platform, without the need to re-authenticate.

Potential benefits for victims of terrorism

- **Faster access to help and entitlements:** Having a "no wrong door" approach that allows victims to register once and be referred for services can facilitate quick and simple connections between victims and service providers, reducing friction and frustration for victims and providers alike.
- **Less repetition, better follow-through:** Secure digital case records that track a user's consent for data-sharing can reduce the need for victims to re-tell their story to multiple providers or enter their intake information multiple times and help providers confirm that referrals lead to support.
- **Stronger surge capacity after major incidents:** Digital portals, hotlines, and messaging-based support can handle spikes in demand, while triage tools can help identify urgent cases that need priority attention.
- **Accessibility-by-design:** The success of multilingual interfaces for government services in India should encourage developers in other areas of the possibility to deliver information and support in local languages and dialects, including via voice, in ways that has transformative potential for reaching victims in low-connectivity and low-literacy settings. While translation is not the same as in-depth cultural fluency, it is an essential starting point that can open many more exciting and low-risk applications in this space.
- **A future platform for long-term, victim-centered support:** With the right safeguards, digital registries and joined-up DPI could make it easier to manage victim services as an integrated infrastructure, rather than one that is siloed between sectors and service providers. This could give victims better access to available services as and when they are needed across a whole spectrum of needs (MHPSS, compensation, justice services, educational support etc.), while giving victims more control over what information is shared, with whom, and why.

Gaps that remain

- **Existing systems don't "talk" to each other by design:** Service providers and government agencies often collect the same information about victims in different formats, making it hard to share referrals, confirm outcomes, and provide a joined-up pathway towards long-term support. Jurisdiction issues can arise over victim registries, especially when they are being collected by different agencies and for different purposes, particularly if victim lists are being used to facilitate an investigation into the incident. At the moment, victim advocates, even those working for local governments, often have to create their own intake methods and conduct needs assessments to recreate these lists to assist victims. Overcoming this barrier to data sharing will be as much a governance challenge as a technical one.
- **Consent, privacy, and trust are hard to get right at scale:** Sensitive victim registries need clear rules on who can access data, for what purpose, and for how long, plus careful, trauma-informed ways of

50 https://victim-support.eu/wp-content/uploads/2021/06/INVICTM-2019-Symposium-Report.pdf#:~:text="When%20you%20are%20a%20victim%20of%20terrorism,Page%2021.%2020%202019%20Strasbourg%20Symposium%20Report.

seeking and updating consent over data usage and sharing with victims. Connecting victim registries to other services and providers also carries additional risks of malicious or inadvertent data leaks and disclosures that will need to be carefully managed. Ensuring that sound technical and data governance principles are in place is a prerequisite to rolling out connected digital victim support systems at scale. To build trust, clear information is needed about user data rights, such as the right to access, correct, or delete data, as well as the strong encryption protocols that are in place to protect sensitive information.

- **Potential misuse of victim data:** In fragile and crisis environments, data privacy and security concerns can peak for communities following an attack. Preventing data-sharing gathered for disaster management from being misused to increase surveillance or track vulnerable communities will require robust safeguards and careful design of systems.
- **DPI may not be developed to work in a crisis environment:** While current DPI discussions focus on steady-state governance, these systems often lack the 'stress-testing' required for the surge-demands and security-critical environment following a terrorist attack. In addition, in the wake of an attack, the risk of malicious targeting of digital systems, information repositories, and the abuse of information about victims may spike, requiring more robust protection than outside of a crisis environment. Internet and power may also be off-line, challenging connectivity and data-sharing. Ensuring that crisis response is considered as a specific use-case during deliberations on the development of DPI is essential.
- **Operational risk and workload:** Digital intake can generate high volumes of incomplete or duplicate reports; automated triage can help but still needs human oversight to avoid errors and potential harm. Additionally, some victims come forward directly after an attack to register and receive support, while others may take many weeks, months, or even years to come forward. Systems need to be designed in a way that allows for the addition, correction, and deletion of records as new information becomes available.
- **Reliance on available data:** All AI-based service referral tools rely on the availability of accurate and timely information about what services are available in the wake of a crisis. While digital data repositories exist on some humanitarian topics such as displacement and natural disasters, for example ReliefWeb or the Humanitarian Data Exchange (HDX),[51] there is no equivalent, trusted source of information that can be used in the immediate aftermath of a terrorist attack, neither for governments nor for victims. Ensuring that there is a digital registry of victim services before a crisis that can be updated rapidly post-incident requires coordination, ownership, and sustainable investment, to ensure that information is comprehensive and updated. Identifying entities that could undertake this role and who would be trusted information-providers for local communities is a task that should precede a crisis.
- **Limited proof of what works:** There are few robust evaluations showing to what extent and under what conditions service referral tools reduce time-to-service or improve longer-term outcomes for users. Finding ways to measure outcomes responsibly and track the long-term benefits of digital triage and information systems is essential to inform future design.

51 https://reliefweb.int/, https://data.humdata.org/

PRIORITY 2

Supporting Justice & Accountability

Digital Chain of Custody

Prosecuting terrorist crimes is a long-term endeavor that often spans decades and multiple international jurisdictions. To ensure that evidence remains trusted and usable years after an attack, pilot projects are exploring how emerging technologies can secure the Chain of Custody: the chronological documentation of evidence. By utilizing blockchain, smart contracts, and homomorphic encryption, legal systems can preserve the integrity of victim testimony and physical evidence across borders.

A secure digital evidentiary lifecycle relies on three interconnected technological building blocks:

- **Verifiable Digital Logs (Blockchain):** A "permissioned ledger" creates an auditable, unalterable trail of how evidence is handled. This ensures that any tampering is immediately visible, preserving the integrity of the data for future court use across different legal jurisdictions.
- **Dynamic Consent (Smart Contracts):** These digital agreements allow victims to set clear, revocable permissions for how their data is used. A victim can authorize their testimony for specific criminal proceedings or for a set period, maintaining agency over their personal information.
- **Secure Evidence Vaults (Homomorphic Encryption):** While the actual files stay in secure institutional vaults, advanced encryption allows authorities to verify or analyze specific parts of a record without exposing the victim's entire personal history or sensitive data on the open internet.

While blockchain-based ledgers offer a "gold standard" for high-integrity evidence, they also require significant operational resources. In resource-constrained settings, simpler high-integrity digital audit trails may be more sustainable. Nevertheless, in the near term, individual elements of this research can be integrated into broader DPI. By ensuring that digital victim registries are built with evidentiary standards in mind from the outset, we can ensure that a victim's initial registration or testimony is compatible with the requirements of a future courtroom, bridging the gap between immediate support and long-term justice.

What could good look like?

For a future prosecutor in a high-resource environment

A prosecutor on a cross-border terrorism case logs into their dashboard and sees a simple checklist the evidence they have, what's missing, and who is allowed to see each item. Every file comes with a built-in history showing who collected it, when it was sealed, and every hand it passed through. A victim's testimony appears with their choices upfront regarding how their statement can be used, who can see it, and for how long. If they withdraw consent later, the system tells the user exactly what they must stop using and automatically alerts anyone else who had access. When the prosecutor shares material with a partner office abroad, they can send only the parts they actually need, with names and personal details hidden by default. Even if a hearing takes place years later, nothing depends on memory or missing files. The prosecution can stand in court and explain, in plain language, how each piece of evidence was handled, backed by a clear, consistent record of victim testimony that cannot be tampered with.

For a future victim in a high-resource environment

A victim sits down with local authorities and shares their testimony. Following the interview, on the screen, they see clear options they can understand: what their statement can be used for, who can see it, and for how long. They choose what feels right today, knowing they can change their mind later. Those choices are saved in the record so everyone involved knows the limits and access can be automatically revoked if the victim alters their consent. When the investigator uploads their statement, their personal details are hidden by default. If their case is shared with another office or another country, they only see what is necessary for their part of the work. The victim gets a simple notification on their portal telling them who asked for access and why. Even years later, they can see what was used, when, and by whom. Their voice is recorded once, handled with care, and used only how they have agreed.

What's currently out there?

- **Chain-of-custody:** The EU-funded LOCARD project created a permissioned-ledger Chain of Custody prototype that moved beyond a purely conceptual paper into a built platform. It provided a proof of concept for a cross-jurisdiction chain-of-custody platform spanning the lifecycle from the collection to the disposition of digital evidence, using a permissioned blockchain and smart contracts as an immutable audit layer, alongside privacy-preserving components to control access to evidence data.[52] In Portugal, studies have examined the potential use of permissioned ledgers to harden the storage of evidence access logs in multi-stakeholder judicial settings.[53]
- **Electronic evidence sharing:** INTERPOL participated in an EU-funded project to enhance international cooperation on the treatment and secure exchange of digital evidence to enhance cross-border judicial cooperation.[54]

52 https://cordis.europa.eu/article/id/442642-blockchain-technology-at-the-service-of-forensic-research https://cordis.europa.eu/article/id/442642-blockchain-technology-at-the-service-of-forensic-research

53 https://www.dpss.inesc-id.pt/~mpc/pubs/Paper_JusticeChain_CoopIS_2019.pdf https://www.dpss.inesc-id.pt/~mpc/pubs/Paper_JusticeChain_CoopIS_2019.pdf

54 https://www.interpol.int/en/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Completed-ICT-law-projects/EVIDENCE2e-CODEX, https://evidence2e-codex.eu/a/evidence2e-codex-end https://www.interpol.int/en/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/Completed-ICT-law-projects/EVIDENCE2e-CODEX, https://evidence2e-codex.eu/a/evidence2e-codex-end

- **Justice-ready standards for DPI:** Research has begun to explore the need for "justice-readiness" to be incorporated into international standards for DPI development, on the basis that considering DPI as purely a service delivery mechanism neglects the potential of its data archives and repositories as a source of accountability and access to justice. Evidentiary standards tend to require specific safeguards to ensure that information is captured and stored in a way that would be admissible in a court of law, and building this in from the start of DPI development is put forward as a way to enhance the contribution of DPI to trust and accountability, as well as information exchange and connectivity.[55]

- **Remote access to courtrooms:** During the trial of the Bataclan attacks in Paris, the French Court of Appeal set up a web radio to allow victims to listen to proceedings remotely.[56] While the lack of translation may have been a barrier for international victims and court proceedings were broadcast without accompanying explanation of the legal aspects of the proceedings,[57] a dedicated psychological assistance line was set up to help victims manage any trauma that was triggered by listening to the trial.

Potential benefits for victims of terrorism

- **Trust-building:** Research and pilots suggest that a permissioned ledger can make Chain of Custody logs harder to retroactively alter and easier to audit across organizations, especially when combined with access controls and the cryptographic anchoring of evidence. This could improve the admissibility of victim testimony in courts even many years after an incident, including if the victim cannot be re-contacted ahead of the trial.

- **Cross-border evidence sharing:** In theory, permissioned ledgers can offer faster, auditable disclosure of evidence to multi-national prosecutorial teams, if data-sharing standards and agreements are in place and evidentiary standards are harmonized.

- **Long-term testimony preservation:** Unalterable records with consent receipts could help ensure that a victim's testimony remains admissible in court even years after the incident, without authorities needing to re-contact the victim. Similarly, victims' interactions with justice or other services could be logged as part of the evidence package to demonstrate the impact of the incident on the victim.

- **Victim-centered consent:** Permissions on how to use their data and testimony could be set by the victims, who can withdraw or amend their consent at any time. Requests to share data across agencies or countries would also be validated by victims themselves.

- **Privacy-by-design:** Homomorphic encryption and other techniques make it easier for partial records to be shared, which could prevent the disclosure or misuse of sensitive information and restrict data-sharing to the essentials for the case.

55 https://www.globalgovernance.eu/publications/justice-ready-digital-public-infrastructure-building-a-third-layer-of-trust-for-democratic-resilience
56 https://www.cours-appel.justice.fr/sites/default/files/2021-08/Vade%20mecum%20WebRradio%202021%2008%2026_0.pdf
57 https://www.justsecurity.org/78126/frances-v13-trial-for-the-2015-paris-terror-attacks-managing-victims-expectations/

Gaps that remain

- **Justice vs. access to justice:** Efforts to improve mechanisms around how evidence is stored and shared and how ongoing proceedings are communicated to victims of terrorism do not inherently improve justice outcomes. Other systemic barriers to justice such as political will, lack of state capacity to prosecute, lack of witness protection, or the lack of an international definition of terrorism, remain challenges faced by victims and their communities.
- **Admissibility and standards:** Courts need to accept ledger logs as evidence for them to be useful. As seen in the LOCARD project, technology often outpaces law. Courts and governments are often slow to accept ledger-based logs, preferring traditional paper-based or centralized digital trails they already trust.
- **Technical limitations:** A blockchain can prove the Chain of Custody log wasn't altered after entry, but it cannot prove the evidence was collected correctly, that a device wasn't compromised, or that humans followed procedure. In addition, privacy and data protection constraints push most systems to store only hashes/metadata on chain. That means the chain-of-custody ledger is only as strong as the linkage between on-chain entries and secure off-chain storage, access control, key management, and retention policies. It should also be noted that technological solutions to support the anonymization of text-based records are currently much more advanced than the anonymization of video or audio footage.
- **Interoperability across borders:** Cross-border cases require shared evidence models and processes. Work in the EU ecosystem on e-evidence exchange (e.g., e-CODEX-related initiatives) underscores how much legal and process harmonization is involved even before adding a ledger layer.
- **The sustainability gap:** The operational cost of maintaining a private blockchain is high. Without long-term funding and dedicated technical expertise, other solutions to improve evidence capture and storage and facilitate cross-border trials may be more effective, particularly in resource-constrained environments.

PRIORITY 3

Protecting Against Revictimization

Virtual Reality (VR) and avatar-based training for First Responders

First responders, including law enforcement, paramedics, and emergency services, are the first point of contact for victims following a terrorist attack.[58] Their initial interactions can have a significant impact on the trajectory of a victim's recovery. While mass-casualty incidents are fortunately rare in many regions, this rarity makes it difficult for personnel to maintain the specialized, trauma-informed skills needed to support victims and families under extreme pressure.

High-fidelity VR and avatar-based simulations are increasingly used to bridge this training gap. By creating hyper-realistic environments, VR allows responders to practice complex tasks such as triage and sensitive interviewing in a safe, controlled setting. Key advantages identified by responders include safe repetition of high-pressure scenarios, the ability to adjust variables, and the ability to receive immediate, data-driven feedback.[59] Long-term knowledge retention and self-reported confidence following VR training is also high, and in some cases is reported to be better with VR than with lectures and live simulations.[60]

As VR and avatar technologies mature, their potential to improve the "human side" of incident response grows. Beyond medical triage, these tools can be used to train service providers in trauma-informed interviewing, helping them gather vital information without causing secondary distress to victims. By prioritizing the lived experience of the victim within the simulation, we can make trauma-informed victim response the standard.

58 First responder is a term that can encapsulate law enforcement, paramedics, emergency responders, firefighters, and other individuals who are deployed rapidly following a terrorist attack, natural disaster or Mass Casualty Incident (MCI).

59 https://pmc.ncbi.nlm.nih.gov/articles/PMC10882557/

60 https://pmc.ncbi.nlm.nih.gov/articles/PMC10882557/

What could good look like?

For a future trainee first responder in a high-income setting

A trainee first responder blocks a few hours to sit down and go through what they have learnt about trauma-informed interviewing with victims and witnesses. They slip on a headset, which loads a street scene after an explosion. A survivor comes into view, in visible distress. They start well, full of reassurance, but soon slip into rapid-fire questioning. The scene cools, the survivor averts their eyes and withdraws. On-screen prompts surface: pause, breathe, ask one open question at a time. The trainee slows down, mirrors the survivor's words, and stops pushing for quick answers. At the end of the simulation, a short debrief shows what helped, what harmed, and offers some tips on how to improve. The trainee repeats the scene with different dialects, ages, and roles (witness, family member, survivor), and then tries different scenarios, building the habit of careful, trauma-informed interviewing under stress. Later, they can go through their metrics and recordings with their assigned coach or draw on a group learning library that uses anonymized examples from teams across the global network.

For a future international police training cohort in a mixed-income setting

A diverse group of senior officers from four continents logs into a secure digital command center. Their mission: coordinate victim response in the immediate aftermath of a simulated blast in a densely populated, low-resource urban hub. The "predictable chaos" of the scenario hits at once: internet infrastructure is compromised, hospital surges are triggering red alerts, and conflicting casualty counts are flooding social media. The team works together to build a strategy to stabilize the panic and track dispersing victims. Satisfied with their plan, they start the live exercise. They must manage distraught family members and frantic health workers under a pressure that feels entirely real. As the "End Exercise" command flashes, the illusion lifts. The officers remove their headsets and adjust their eyes to the light of their own home offices. They weren't in a physical mock-city, but a digital twin populated by digital avatars. Their performance metrics, from the speed of health service mobilization to the empathy shown in crisis communication, are instantly tabulated. They spend the final hour in a cross-border debrief, reviewing the 3D playback of their decisions and refining a global standard for victim management that can be deployed anywhere in the real world.

What's currently out there?

- **VR police training exercises:** Projects like the EU-funded SHORTPROS used VR training and integration with smart vests and other monitors to improve outcomes of police training for high stress operational environments. Findings validated VR training's utility for recreating accurate stress environments, allowing trainees to practice skills to maintain high performance under pressure, and providing unique opportunities to discover and embed correct decisions and actions.[61] A range of studies have been conducted to test the training outcomes of VR-based training for first responders for mass casualty incidents and trauma room applications, showing positive outcomes even in comparison to traditional in-person training methods.[62]

61 https://cordis.europa.eu/project/id/833672, https://www.mdpi.com/2414-4088/7/2/14 https://cordis.europa.eu/project/id/833672, https://www.mdpi.com/2414-4088/7/2/14

62 https://link.springer.com/article/10.1186/s13584-025-00681-9, https://link.springer.com/article/10.1186/s12909-025-07319-z?fromPaywallRec=false, https://link.springer.com/article/10.1186/s12909-024-05764-w, https://dl.acm.org/doi/fullHtml/10.1145/3641825.3687707#BibPLXBIB0003 https://link.springer.com/article/10.1186/s13584-025-00681-9, https://link.springer.com/article/10.1186/s12909-025-07319-z?fromPaywallRec=false, https://link.springer.com/article/10.1186/s12909-024-05764-w, https://dl.acm.org/doi/fullHtml/10.1145/3641825.3687707#BibPLXBIB0003

- **Immersive online tabletop exercises (TTX) on victim response:** In 2021, constrained from doing a live exercise by the COVID-19 pandemic, a joint UK/Canada online TTX was organized to test two police agencies' victim responses in a terrorist attack scenario. Character development drew on the real and diverse experiences of victims and survivors and highlighted different victim and first responder profiles to encourage participants to see the victims as individuals that reacted to the impact of the attack in diverse ways. The TTX integrated realistic images, video footage, and audio content to create an immersive testing environment. A report summarizing the TTX and providing lessons learned for others who are interested in planning similar exercises was produced by UK National Police Wellbeing Service (Oscar Kilo) and The International Network Supporting Victims of Terrorism and Mass Violence (INVICTM).[63]

- **Victim avatars for trauma-informed training:** Training platforms like OSACO's EchoMind are already developing and piloting AI-powered avatar training on trauma-informed interviewing techniques for first responders, with demonstrated results around trainee's increasing use of open-ended questions and evidence-based rapport-building following platform use.[64]

- **Testing with vulnerable populations:** Results on the applicability and utility of VR-based training for practitioners working with particularly vulnerable witnesses such as child abuse victims also show positive results when the VR environments are fully immersive and trained on real interview data, an improvement on computer-based or 2D avatar simulations.[65] Video-based training on trauma-informed interview techniques for survivors of sexual violence that incorporates commentary from trauma experts and survivors has also been used in Canada to help police officers apply knowledge on how trauma affects victim testimony to their engagement with victims.[66]

- **In-person victim-centered police training exercises:** The idea of using live exercises and scenarios to map out victim response as part of incident management planning is not new. The FBI runs victim services exercises under its ELEVATE program,[67] the New York State Office of Victim Services (OVS) and the Global Center for AI in Mental Health at the University at Albany have partnered to offer Disaster Mental Health Preparedness Trainings to victim service professionals from OVS-funded organizations,[68] Canada has developed the Canadian Framework for Trauma-Informed Response in Policing,[69] while the International Association of Chiefs of Police (IACP) serves as the training and technical assistance provider for a Law Enforcement-Based Victim Services and Technical Assistance Program.[70]

Potential benefits for victims of terrorism

- **Safer practice for difficult conversations:** Learners can make mistakes without harming real victims and survivors, then immediately retry with feedback. By the time they are responding to a real crisis, they are more likely to be confident and capable of treating victims in a trauma-informed and sensitive way, improving the support they can offer even under intense stress.

- **Greater empathy between victims and responders:** Spending more training time on victim response, or trauma-informed interviewing, can help build a better understanding between victims and responders. Understanding the theoretical impacts of trauma on victim recall is different to seeing it consistently in your training and coming equipped with the tools and the understanding to safely interact with victims in a crisis environment.

63 https://victim-support.eu/wp-content/files_mf/16533986082022InternationalCTTTXReport.pdf

64 https://www.osacogroup.com/usa/, https://www.osacogroup.com/echomind-ai-interview-training/ https://www.osacogroup.com/usa/, https://www.osacogroup.com/echomind-ai-interview-training/

65 https://www.frontiersin.org/journals/virtual-reality/articles/10.3389/frvir.2025.1550907/full

66 https://www.cbc.ca/news/canada/thunder-bay/trauma-informed-police-training-opp-1.6706163

67 https://www.fbi.gov/news/stories/fbi-course-elevates-victim-services-102519#:~:text=%E2%80%9CThe%20whole%20idea%20is%20to,where%20their%20loved%20ones%20are.

68 https://www.ovsacademy.com/

69 https://www.oacp.ca/en/news/new-trauma-informed-response-resource.aspx#:~:text=The%20Canadian%20Framework%20for%20Trauma%2DInformed%20Response%20in,Annual%20General%20Meeting%20on%20July%2025%2C%202022.

70 https://www.theiacp.org/projects/law-enforcement-based-victim-services-lev

- **Consistency at scale:** Consistent feedback metrics like the ratio of open-ended questions asked or the number of times a trainee interrupts a victim can raise the baseline across agencies and provide a tangible way to track training progress over time.
- **More opportunities to train:** Live exercises and in-person training are important resources and are critical for first responders and service providers operating in crisis contexts. They are, however, relatively expensive to run and require a significant amount of expertise on the part of the facilitators and actors to recreate realistic scenarios and victim perspectives. Digitizing some forms of this training could allow police forces and other organizations to run more frequent training or ensure that on-demand resources are available to reinforce skills in between live training exercises, resulting in better outcomes for responders and victims alike.
- **Potential integration into security force assistance programs and packages:** International trainers can serve as the hosts for virtual exercises, or access to digital training platforms could be sponsored by an international donor to widen access in countries most affected by terrorism to improve the support that more victims receive.

Gaps that remain

- **Guardrails for non-leading questions:** Systems need robust detection and feedback for suggestive prompts, interruption, and over-questioning under stress. The use of AI-enabled analytics unlocks enormous potential but needs to be tailored to different linguistic and cultural norms.
- **Technical issues:** When VR and avatar-based environments freeze, glitch, or do not have an intuitive user interface, they become less effective training tools. While demos and tutorials can overcome some of these challenges, ensuring stable training environments even in low-connectivity settings will be key to ensuring the global suitability of these tools.
- **Limited victim engagement in tool design:** Work is needed with victims' groups to ensure that AI-powered avatars do not inadvertently rely on stereotypes and that the 'distress cues' modeled by AI accurately reflect the diverse psychological realities of victims and survivors.
- **Content validity and transfer:** Many scenarios measure process indicators, but fewer demonstrate real-world transfer of interviewing quality or reduced harm to victims and survivors. Longer-term examination of the potential real-world performance benefits of virtual training is needed.
- **Psychological safety for trainees:** Immersive scenes can distress learners; programs require opt-outs, graded exposure, and screening. Integrating psychological check-ins with trainees and ensuring that their psychosocial reaction to training is monitored, is important.
- **Security concerns:** Privacy leakage from training systems or unauthorized edit access to training environments could leave trainees vulnerable. Tampering with a system to influence the likely ethnicity of a perpetrator, to cause sensory harm to users, or to manipulate behavior could be difficult to detect. Data privacy of sensitive personal training footage will also need protecting and safeguarding.
- **Adoption issues:** Designing tools for police forces, first responders, and government agencies can be challenging, as solutions need to map against existing procurement requirements and training cycles. Close engagement with the agencies intended to use the tool, or co-design with potential users, is essential to remove barriers to adoption.
- **Accessibility and cost:** While the cost of headsets is reducing, training platforms and avatars still cost money to develop. Innovative financing mechanisms, the integration of virtual tools into international assistance packages, and other solutions are important to ensure that the benefits of virtual training are not concentrated only in high-resource contexts.

Tools and approaches to counter mis-/disinformation

The immediate aftermath of a terrorist attack is a high-stakes information environment. While online platforms have matured their crisis protocols to limit the circulation of extremist and graphic content, victims remain uniquely vulnerable to secondary trauma from a variety of online sources. Protecting victims and survivors requires a sophisticated blend of platform policy and trauma-informed moderation.

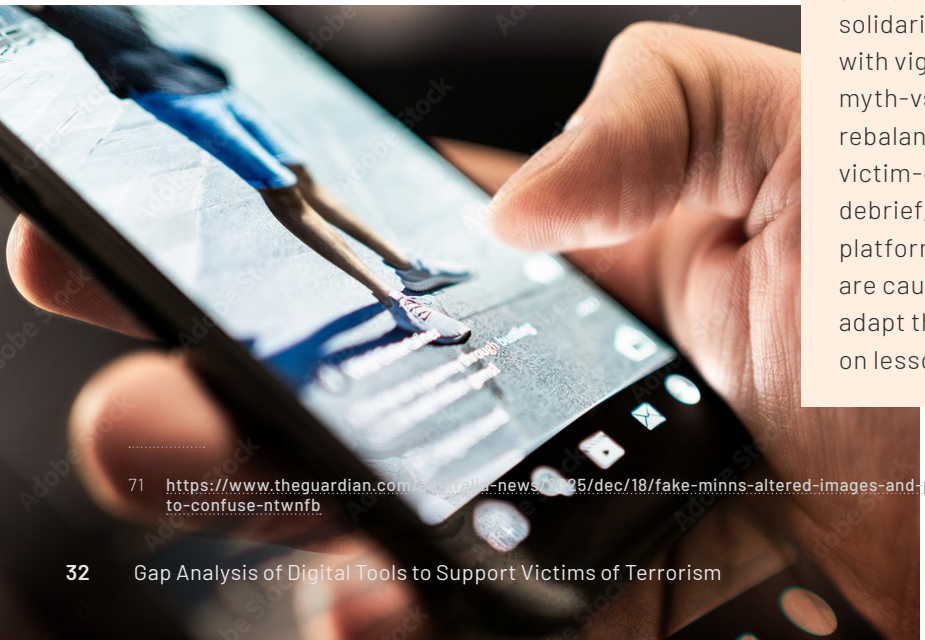
A growing and disturbing trend involves the use of AI-generated mis-/disinformation to undermine the credibility of victims. For example, following the December 2025 Bondi Beach attack, faked images of real victims were circulated depicting them applying fake blood.[71] This type of targeted disinformation can be deeply traumatic for victims and their communities, hindering both personal healing and public trust. A key consideration for companies working in this space is that legal content, such as bystander footage, images of deceased loved ones, deepfakes of victims, or the malicious release of personal information about victims ("doxxing"), can be as psychologically damaging to victims as illegal content such as extremist content. Current moderation often fails to capture these nuances, especially when the harmful content is not graphic or violent in nature.

This section explores how platforms and regulators can ensure that crisis response mechanisms explicitly recognize the specific vulnerabilities of victims, moving beyond simple "takedowns" toward a more protective digital ecosystem.

What could good look like?

For a future cross-sectoral crisis communications team

Within the first hour after the attack, the state police media unit, the city's emergency management team, and a victims' association activate a pre-agreed "mis-/disinformation response room" with major platforms. A single, fast-updating public page goes live: verified facts, what's still unknown, and a clear request not to share graphic footage or unverified leaks. The victims' association adds a short, trauma-informed note: "seeing fakes can retraumatize; you're not alone; here's where to get support." Platforms switch to "crisis mode" so AI assistants stop speculating and only summarize information about the attack from vetted sources. A few hours later, a manipulated image starts trending, falsely depicting a survivor faking their injuries. Platform integrity teams run provenance checks and confirm the image is synthetic; where available, watermark detection tools help attribute AI-generated content to the originating model family, enabling faster action. The image is labelled and downranked, duplicates are matched via hashing, and accounts pushing it at scale are frozen. Meanwhile, trained community content monitors (local NGOs, victims' associations, and trusted volunteers) feed falsehoods into a shared queue for rapid review. Neighborhood groups and local leaders receive ready-to-share solidarity cards created by victims' associations with vigil information, donation guidance, and myth-vs-fact slides so the community can help rebalance coverage towards trauma-sensitive, victim-centric content. In the post-incident debrief, victims' voices are heard so that platforms are aware of the types of content that are causing the most distress, so that they can adapt their content moderation policies based on lessons learned.



71 https://www.theguardian.com/australia-news/2025/dec/18/fake-minns-altered-images-and-psyop-theories-bondi-attack-misinformation-shows-ais-power-to-confuse-ntwnfb

What's currently out there?

- **Post-incident content moderation:** Spain's Centre of Intelligence to Counter Terrorism and Organized Crime is working with victims on the process of defining and removing harmful content from social media. A dedicated team is responsible for ensuring that not only misinformation but any material that may lead to victims' retraumatization is addressed and removed.
- **Reliable crisis comms:** During COVID-19, the Government of India partnered with Haptik, a start-up, to build the MyGov Corona Helpdesk in just five days to help communities get reliable multilingual information on the pandemic and counter common myths and misinformation.[72]
- **Digital authenticity checkers:** Tools such as the Austrian Institute of Technology's "defalsif-AI" platform use AI to analyze digital content for authenticity, including text, images, videos, and audio. This can help to identify false materials, including deepfakes, which could help to speed up their identification and take-down in a crisis setting.[73]
- **Platform-level content credentials:** Platforms use a mixture of model-specific watermarks and content credentials to identify content as AI-generated or AI-edited. For example, Google uses a hidden watermark called SynthID embedded in content created on or modified by Google models.[74] This was used following the terrorist attack on Bondi Beach, Australia, in December 2025 to confirm that purported images of the perpetrator that were circulating were AI-generated.[75] OpenAI attaches a C2PA manifest (signed metadata) to images generated via its models and API so that people can check it via verification sites like Content Credentials.[76] Platforms can also verify via their internal generation logs, content hashes, and model-origin classifiers trained to recognize patterns typical of different model families.
- **AI-enabled misinformation detection:** Microsoft's AI for Good Lab, in collaboration with Princeton University's Empirical Studies of Conflict Project, has experimented with training models capable of identifying unreliable sites based on patterns of ingoing and outgoing traffic, with potential practical applications for identifying new misinformation sites at scale.[77]
- **Extremist content takedowns:** The Global Internet Forum to Counter Terrorism (GIFCT)[78] has grown from four founding members (Facebook, Microsoft, X and YouTube) to a network of thirty-three technology platforms who maintain a hash-sharing database and Incident Response Framework (IRF). This allows for the sharing of "hashes" or digital fingerprints of identified extremist content to be shared between platforms, speeding up the identification and takedown of visually similar material without sharing user data between companies. Since the livestreaming of the 2019 terrorist attack in Christchurch, New Zealand by the perpetrator, 24 further livestreams of attacks or circulation of attack footage have resulted in the activation of an IRF.[79] The Christchurch Call Crisis Response Protocol was developed in the aftermath of the 2019 terrorist attack,[80] initially focused on perpetrator or accomplice-produced content and since expanded to cover bystander and CCTV footage, and also AI-generated content.[81] In 2024, Tech Against Terrorism expanded its Incident Response Process to become a 24/7 operational capacity that can work to alert content to tech platforms and relevant authorities faster. It also has Emergency Response Teams that can be deployed to enable round-the-clock reactive assessment and referral of terrorist content online after terrorist attacks.[82]

72 https://www.haptik.ai/resources/case-study/govt-of-india

73 https://www.ait.ac.at/en/research-topics/surveillance-protection/projects/defalsif-ai

74 https://deepmind.google/models/synthid/

75 https://www.abc.net.au/news/2025-12-18/verify-disinformation-and-deepfakes-after-bondi-attack/106154250

76 https://help.openai.com/en/articles/8912793-c2pa-in-chatgpt-images, https://openai.com/index/understanding-the-source-of-what-we-see-and-hear-online/, https://verify.contentauthenticity.org/ https://help.openai.com/en/articles/8912793-c2pa-in-chatgpt-images, https://openai.com/index/understanding-the-source-of-what-we-see-and-hear-online/, https://verify.contentauthenticity.org/

77 https://files.osf.io/v1/resources/x4dh7/providers/osfstorage/6487b927a31091009ad10d0a?action=download&direct&version=1 https://files.osf.io/v1/resources/x4dh7/providers/osfstorage/6487b927a31091009ad10d0a?action=download&direct&version=1

78 https://gifct.org/

79 https://gifct.org/incident-response-activity/

80 https://www.christchurchcall.org/responding-to-crises/

81 https://www.christchurchcall.org/what-does-our-updated-crisis-response-protocol-actually-do/

82 https://techagainstterrorism.org/news/tech-against-terrorism-expands-its-terrorist-content-alerting-system-to-24/7-emergency-response-team-with-support-from-the-australian-government

- **City and community-led crisis communications guidance:** Resources such as the Institute for Strategic Dialogue (ISD)'s Strong Cities Network's Guide to City-Led Response outline the considerations and tools for crisis communications, including addressing mis-/disinformation and supporting communities that may become targets of hate crimes following an attack.[83]
- **Violence prevention services:** Organizations like Moonshot signpost violence prevention services directly to bystanders and people consuming violent content online.[84] Parents for Peace provides tools to support those who are concerned that a loved one is considering violent action, including via their helpline, peer support services, and links to community-based support.[85] Research initiatives such as the Polarization and Extremism Research and Innovation Lab at the School of Public Affairs at the American University in Washington DC, seek to create effective violence prevention tools and resources while centering the needs of targeted groups, victims, and survivors.[86]
- **Platform policies:** Platforms have established several mechanisms to stabilize the information environment post-incident. Major platforms maintain policies against terrorist/violent-extremist content and violent/graphic content, enforced via a mix of automated detection, human review, user reporting, and "visibility controls" (labels, downranking, age-gating). In some jurisdictions legislative tools and bodies enforce the removal of illegal content (including terrorist content) and crisis response mechanisms, for example the EU Digital Services Act (DSA), the UK Online Safety Act, and Australia's eSafety Commissioner. In the EU, the 2022 Code of Practice on Disinformation was endorsed for integration with the DSA.[87]
- **Regular reporting:** Tools such as Google's Transparency Report give statistics for platforms like YouTube on numbers of videos removed for categories such as misinformation (over 100,000 between July-September 2025) or promotion of violence or violent extremism (over 361,000 between October-December 2025) and sources of first detection (automated flagging, users, organizations, government agencies).[88]

Potential benefits for victims of terrorism

- **A safer online environment:** Reduced exposure to perpetrator propaganda and hate, limiting retraumatization and copycat risk. Lowering victims' exposure to harmful content in the immediate aftermath of an attack or around prominent anniversaries and commemorations could help to promote healing and recovery and remove a potential source of additional trauma.
- **Access to information:** Removing and reducing the proliferation of deepfakes and mis-/disinformation can boost victims' and communities' access to trustworthy, victim-safe information for families and communities, as an essential part of crisis response and crisis communications.
- **Community-led communications:** Stronger social cohesion can be promoted through proactive, localized engagement and transparency on information circulating following an attack. Involving victims' associations, community representatives and experts in the crisis communications response can help to build trust in the information and reduce tensions.
- **Victim-centered attack coverage:** The amplification of victims' voices and decentering of extremist and explicit content following an attack can help to ensure that affected communities are not overshadowed or overtaken by harmful speculation as to the motivations and identity of the perpetrator(s).

83 https://strongcitiesnetwork.org/resource/a-guide-for-city-led-response/4/
84 https://moonshotteam.com/online-violence-prevention/
85 https://www.parents4peace.org/
86 https://perilresearch.com/
87 https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
88 https://transparencyreport.google.com/youtube-policy/removals

Gaps that remain

- **The hardest problem is "novel, high-velocity, context-dependent" content:** Hashing works best for duplicates of known items; it is less effective for new manipulated content, live streams, rapidly edited clips, and "borderline" material where intent and newsworthiness matter. GIFCT itself highlights the need to continually evolve definitions and inclusion parameters as tactics and content types change.
- **Over-removal vs under-removal:** Platforms lean heavily on automated systems of content removal for speed, but errors still occur, sometimes at scale, through misclassification or ranking glitches that expose users to harmful graphic content even when settings are enabled. On the other hand, the wholesale removal of online content that is not illegal in nature but may be harmful poses important legal questions around freedom of speech and must be carefully managed.
- **Crowd-based corrections often arrive too late for "breaking news.":** Even where Community Notes can reduce engagement, multiple analyses and recent incident coverage argue that corrections frequently trail viral spread, especially during crises, so the harm is front-loaded.
- **Fragmentation and uneven capacity across the ecosystem:** Large platforms may have sophisticated integrity teams; smaller services, fringe platforms, and encrypted/private channels often have weaker tooling, fewer reviewers, and less consistent participation in voluntary schemes, creating displacement rather than resolution of harmful content.
- **Difficulties for victims and associations to advocate with large platforms:** Negotiating with online platforms and frontier labs to ensure safeguards around creating, spreading, and amplifying content that can be harmful to victims is difficult for individual victims' associations or national governments, and requires joined-up, evidence-based advocacy.
- **Easier treatment of mis-/disinformation and illegal content than 'harmful' content:** It is vital to distinguish between false content and harmful content, which may be accurate but contain graphic or identifying footage. While technical tools like C2PA can prove an image is 'real,' they do not address the trauma caused by the circulation of that real image.
- **Victims' needs change over time:** While high-profile coverage and advocacy may be welcomed by victims in the immediate aftermath of an attack, these views may shift over time. For example, families advocating for the release of loved ones being held by terrorist groups may seek wide media coverage but then may wish to reclaim privacy once their loved one is released. The opposite can also be true, with victims feeling overwhelmed or unprepared to talk to media in the immediate aftermath of an attack but seeking to share their stories later. Different victims will have unique needs and concerns, making it hard to produce consistent rules around what harmful content looks like, outside of common standards around extremist content or mis-/disinformation, and greater work with victims' groups to understand their needs and perspectives is important.
- **Engaging in content moderation can also cause harm:** When thinking about how best to integrate victims' perspectives into incident response cycles, it is important to consider the potential psychological impact on victims of collecting, viewing, and sharing harmful content. It is more appropriate to work with established victims' associations, civil society organizations, or victim volunteer responders from prior attacks who can leverage their past experiences and lessons learned, rather than trying to engage directly with the victims of the incident that is unfolding. Integrating these groups into post-incident debriefs rather than real-time content monitoring may also carry lower retraumatization risks.

PRIORITY 4

Supporting Victim Empowerment & Agency

Digital platforms for peer-to-peer support and learning

For victims of terrorism, digital spaces offer a uniquely powerful resource: connection without geographic constraints. When built on a foundation of rigorous governance, these platforms reduce isolation, normalize help-seeking behavior, and provide a repository of "lived experience" knowledge that is often more accessible than formal, in-person services.

The greatest potential for these platforms lies in moving beyond simple message boards toward integrated recovery ecosystems. These environments combine community belonging with practical, evidence-based tools, guided courses, coping exercises, and step-by-step resources that can be accessed at their own pace.

In trauma-affected communities, the intersection of community, learning, and safety is what makes digital support sustainable. By enabling victims from conflict-affected or remote regions to connect with peers who share similar experiences, regardless of their physical location, these platforms empower victims to navigate their recovery with a sense of collective resilience and restored agency. Sustainable engagement depends on a combination of privacy-by-default, clear behavioral boundaries, and active, trauma-informed moderation to prevent re-traumatization.

What could good look like?

For a future victim with access to the internet

It has been a few years since the attack, but the memories come rushing back one morning when a victim's phone flashes with a news alert of an attack in another city. The victim feels shaken, and when a counsellor mentions a survivor-led online community for victims of terrorism, they ask for the link. From the outset the platform feels reassuring. After verifying their identity with the moderators, all their personal details remain private. A short introductory video shares the code of conduct: this is a safe space where conversations must remain respectful, and members support each other. There are weekly small-group meetings organized by victims and survivors, and a small library of bite-sized lessons and tools including on grounding exercises, navigating compensation systems, dealing with anniversaries, returning to work. A pinned post reminds everyone: Share what you wish, skip what you don't. For a few weeks, they do not feel comfortable posting. Then one night they write on the chat board, "Does anyone else feel like their body is still bracing for impact?" Within minutes, three replies arrive, not advice, just recognition. Weeks later, they are not "over it." But they are no longer alone with it.

What's currently out there?

- **Digital platforms for victims of terrorism:** UNOCT-hosted communities such as the Victims of Terrorism Associations Network (VoTAN) have a digital space on the UN's Connect and Learn platform,[89] which provides an invite-only space for members to connect, post events, share resources, provide peer-to-peer support, and stay up to date with each other's activities.
- **Online peer support for victims of mass violence:** In the United States, there are multiple initiatives that offer online peer support for victims of mass violence, such as the Rebels Project[90] and the HEART Peer Support Program.[91] There are monthly online meetings hosted by the S.T.O.P. Coalition (Survivors of Tragedy Outreach Program),[92] and monthly groups for resiliency center directors and navigators hosted by the National Mass Violence Center (NMVC),[93] to mention a few.
- **Peer support mental health platforms:** In the UK, digital platforms like Togetherall (previously the Big White Wall) are offered in partnership with the National Health Service through different councils, employers, universities or colleges.[94] The site offers digital mental health support services including peer support, community discussion groups, anonymous meetings to share experiences, MHPSS learning resources, and access to professional support, including for those struggling with PTSD. Digital platforms like "7 cups" can connect people struggling with a broad range of mental health concerns with a community of trained 'listeners' and members, giving people access to peer support, professional support, and education programs.[95]
- **Peer support digital health services:** Platforms like "Patients like Me" connect people to peer support, personalized health insights, tailored digital health services and patient-friendly clinical education to build a community of patients who can support each other through their health and treatment journey.[96]

Potential benefits for victims of terrorism

- **Safe peer-to-peer connection and mutual aid across borders:** A trusted space can reduce isolation, normalize reactions to trauma, and create pathways for practical support, especially when local options are limited.
- **Rapid coordination after incidents:** Digital spaces can support surge communication in the immediate aftermath while helping victims avoid harmful rumor cycles and retraumatizing content elsewhere online.
- **Durable knowledge exchange and victim-led learning:** A well-structured platform can act as a living library of survivor expertise on topics including rights and entitlements, compensation processes, dealing with anniversaries, returning to work/school, parenting after loss, media engagement, and self-care.
- **Greater opportunities for collaboration and advocacy:** Communities can form working groups (e.g. youth, family members, disability inclusion), coordinate joint statements, share best practices in victim assistance, and strengthen victim-led advocacy with less reliance on travel and formal conferences.
- **Continuity of support over time:** Unlike time-bound projects, a digital community can be more able to sustain support through long recovery arcs and life transitions, offering ongoing connection and educational opportunities as needs evolve.

89 https://www.un.org/counterterrorism/en/events/launch-victims-terrorism-associations-network-votan
90 https://www.therebelsproject.org/
91 https://resiliencyandjustice.org/heart/
92 https://www.thestopcoalition.org/
93 https://nmvvrc.org/
94 https://togetherall.com/en-gb/big-white-wall/
95 https://www.7cups.com/about/
96 https://www.patientslikeme.com/about

Gaps that remain

- **Sustained moderation and trauma-informed governance at scale:** Maintaining quality, consistency, and safeguarding is resource-intensive; clear escalation pathways, duty-of-care boundaries, and moderator wellbeing support are essential. Developers may need to incorporate features, or else moderators must define procedures that allow users to report abuses, monitor compliance with international human rights standards, and work towards the prevention of future violations.
- **Privacy-preserving discovery and participation:** Victims may need to find support without exposing identity, location, or affiliations; designing for pseudonymity, minimal data collection, secure communications, and safe "read-only" engagement remains challenging.
- **Language coverage and cultural adaptation:** Supporting smaller languages/dialects and culturally specific expressions of grief, faith, and coping is difficult; translation alone is not enough without locally informed moderation and content.
- **Safety in adversarial environments:** Platforms can be sources for harassment, extremist infiltration, doxxing, or disinformation; robust trust-and-safety and anti-abuse tooling are ongoing needs.
- **Potential for harm:** Sustained engagement with digital tools can itself be a source of trauma, including via unwanted push notifications about an attack, algorithmic amplification of attack-related content, and the emotional burden of maintaining a presence on a platform that constantly surfaces painful memories.
- **Representation and inclusion:** Digital spaces can over-represent those with connectivity, literacy, and confidence; deliberate outreach and accessible design are needed to include other groups including older victims, persons with disabilities, and those in low-connectivity contexts.

Digital resilience tools

In the wake of a terrorist attack, the digital world is often the first place where a survivor's story is told, frequently without their consent. While platform moderation is vital, a critical gap remains in supporting the active digital agency of those affected. Victims are not passive subjects of online content; they are individuals navigating a challenging information ecosystem while managing profound trauma. Digital resilience refers to the tools and frameworks that empower victims and survivors to reclaim their narratives and protect their digital footprints.

For example, in the initial stages of a crisis, families and victims may need structured protocols to manage a sudden surge of global attention or to coordinate messaging during a campaign for a loved one.

As the transition from crisis to recovery unfolds, these needs evolve into a requirement for trauma-informed posting practices, boundary-setting with the media, and the ability to manage public-facing accounts without inviting secondary trauma.

True empowerment in the digital age involves ensuring victims have the digital literacy to identify when their experiences are being appropriated and the technical means to seek the removal of content that distorts their reality. By integrating these tools into the recovery journey, we ensure victims can navigate the online world with dignity and safety.

What could good look like?

For a future peer-to-peer network of victims and survivors with access to the internet and messaging services:

As news breaks of a major terrorist attack, members of a global survivor network alert each other on their group chat and re-share the link to their shared digital resilience toolkit. One member quickly downloads the "First 48 Hours" checklist, sharing a verified, trauma-informed "Pause Before You Scroll" graphic into their local WhatsApp groups to alert victims to the coming wave of graphic and potentially traumatic content, whether real or faked. As the information ecosystem becomes flooded with speculative theories, the network uses a pre-prepared Verification Primer to help their own families and communities understand how algorithms are amplifying the most graphic content. They use pre-vetted templates to coordinate "Stop the Share" messages across their personal social feeds, protecting the dignity of the new victims while signposting official, secure information sources. Acknowledging the psychological toll of this work, the group also accesses and shares hints and tips to manage members' own exposure, recalling breathing space exercises and links to peer-support and specialist services. By sharing these tools laterally, the network can reach victims, families, and communities in crisis while also protecting their own mental health and digital resilience.

What's currently out there?

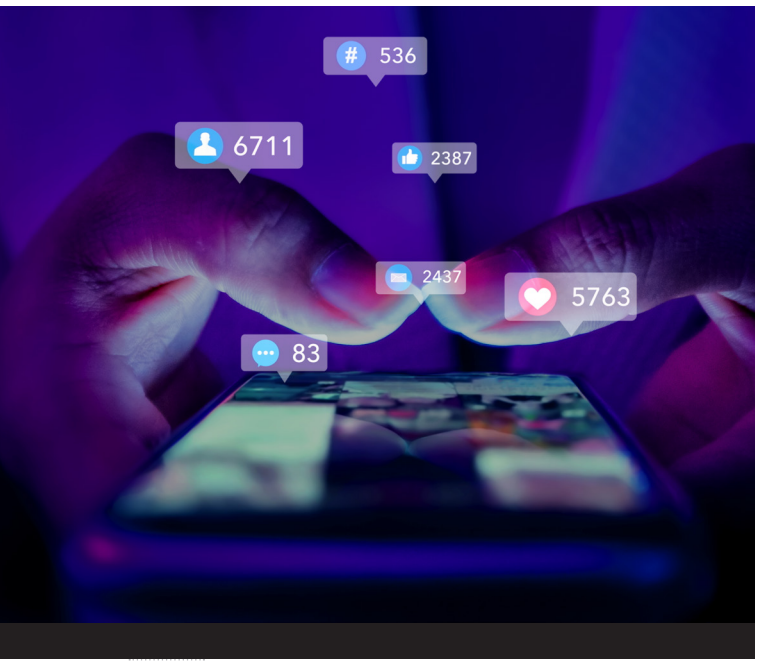
- **Victim-centered media and privacy guides:** Organizations like the US National Center for Victims of Crime (NCVC) and Victims Services (Australian NSW Government) provide structured frameworks for victims to navigate media interactions.[97] These resources offer practical advice on maintaining privacy and dignity while ensuring that if a victim chooses to speak, they do so on their own terms.
- **Media readiness and interview preparation:** The US National Mass Violence Center (NMVC) offers specialized toolkits to help victims prepare for the unique pressures of news interviews.[98] These guides focus on trauma-informed communication, helping individuals decide when and how to engage with journalists after an incident or during sensitive anniversaries.
- **Ethical journalism and reporting frameworks:** International bodies like the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Czech Ministry of Interior have developed handbooks and psychosocial guidelines specifically for journalists.[99] These tools aim to encourage reporters to adopt practices that prevent re-traumatization and respect the psychological state of victims during crisis and disaster coverage.
- **Ethical technology and computing curricula:** The Mozilla Foundation hosts the Responsible Computing Challenge, which supports the conceptualization, development, and piloting of curricula and tools that encourage computing and technology students to integrate ethics, accountability, and inclusivity in their design. WebEase was developed as part of the Responsible Computing Challenge in India and consists of an open-source lightweight accessibility conversion layer that can improve the accessibility of existing digital tools without needing full redevelopment. This could be used to make a range of existing digital services more accessible to victims of terrorism with specific visual, auditory, or cognitive requirements.[100]

97 https://victimsofcrime.org/media-ethics/, https://angelhands.org.au/wp-content/uploads/2017/12/A-guide-to-media-for-victims-of-crime.pdf
98 https://nmvvrc.org/media/ujbbwx2k/preparing-for-news-media-interviews.pdf,
99 https://unesdoc.unesco.org/ark:/48223/pf0000247074, https://mv.gov.cz/mvcren/article/psychosocial-support-guidelines.aspx?q=Y2hudW09Mw%3D%3D
100 https://www.mozillafoundation.org/en/responsible-computing-challenge/

- **Strategic communication and perception mapping:** Victim Support Europe and the Radicalisation Awareness Network (RAN)'s Victims of Terrorism Working Group have established strategic frameworks to transform how victims are perceived in the public eye.[101] Their work focuses on moving away from "victimhood" narratives toward empowerment, ensuring that communication from authorities and media alike is respectful and inclusive.

- **Victim-led recommendations on victim-centered media and social media coverage:** Survivors Against Terror has conducted targeted research into the impact of media intrusion on victim well-being and has a set of guidelines for victim-centered media coverage of attacks,[102] and responsible social media usage following an attack.[103]

- **Advocacy for "No Notoriety.":** Campaigns like No Notoriety focus on the digital ecosystem, pushing for the responsible handling of perpetrator information to deny them the "fame" they seek. These initiatives empower victim communities to advocate for media standards that prioritize the needs of victims over the sensationalism of the attack.[104]



Potential benefits for victims of terrorism

- **Restored agency and digital autonomy:** Providing victims with the tools to safely navigate the digital sphere in real-time can foster a sense of control and agency that is often stripped away in the aftermath of an attack and can prevent retraumatization from occurring.

- **A "collective shield" for mental health:** Rapid-response toolkits allow victims' associations to mobilize instantly, sharing "pause before you scroll" advisories that prevent members from being blindsided by graphic or retraumatizing footage. This peer support system reduces the risk of secondary trauma and promotes long-term psychological resilience.

- **Countering a focus on perpetrators over victims:** Ready-to-go templates and "No Notoriety" protocols help victims to collectively decenter the perpetrator's narrative. By focusing digital traffic on victim solidarity and verified facts, communities can effectively starve extremist content of the oxygen it needs to spread.

- **Global accessibility of trauma-informed care:** Digital resilience tools can be adapted across different languages and cultural contexts, ensuring that victims in low-resource or geographically isolated settings have the same access to high-quality, survivor-led guidance as those in major urban hubs.

- **Empowered advocacy and narrative control:** When victims are equipped with clear frameworks for media engagement and digital literacy, they can shape how their stories are told. This ensures that the public memory of an event is rooted in the dignity and lived experiences of those affected, rather than in harmful speculation or misinformation.

101 https://home-affairs.ec.europa.eu/system/files/2022-08/ran_paper_vot_perception_of_vot_in_media_23-24052022_en.pdf, https://victim-support.eu/wp-content/files_mf/1681918001TransformingHowWeCommunicateWithVictims_compressed.pdf

102 https://survivorsagainstterror.org.uk/wp-content/uploads/2023/01/Media-Report-Oct-2021-A-Second-Trauma-5.pdf

103 https://survivorsagainstterror.org.uk/wp-content/uploads/2025/11/Social-media-report.pdf

104 https://nonotoriety.com/

Gaps that remain

- **Co-design and sustainable victim-led governance:** While the potential for victim-led tools is high, the reality of maintaining them is resource-heavy. There is a persistent gap in providing the long-term funding and technical support needed for victims' associations to develop and evolve strategic communications content to match the pace of change in the digital environment. Ensuring these tools remain "by victims, for victims" requires durable partnerships that don't vanish after the initial development phase.
- **Risk of harm:** Empowering victims to take a more active role in the digital space can be a pathway to healing, but also to burnout. Enabling networks of victims and victims' associations to provide rapid guidance to their communities in the wake of an attack or to raise their voice as global advocates comes with risks to their own mental health, and it should be acknowledged that they do not hold the ultimate responsibility for creating a safe digital environment.
- **Verification at the speed of generative AI:** As deepfakes and AI-generated misinformation become more sophisticated and faster to produce, the gap between a "viral lie" and a "verified truth" is widening. Victim networks need more than just manual checklists; they require accessible, real-time AI detection tools or partnerships with platforms that can verify and take down information at speed to keep pace with the 2026 information landscape.
- **Cultural nuances beyond simple translation:** A "one-size-fits-all" digital resilience tool risks failing in diverse global contexts. There is a significant gap in adapting these tools to reflect localized expressions of grief, religious sensitivities, and varying levels of trust in state authorities. True digital resilience requires content that is culturally resonant, not just linguistically accurate.
- **Inclusion for offline and low-literacy contexts:** There is a risk that high-tech digital resilience tools favor those with high connectivity and tech-savviness. A persistent gap remains in ensuring that older victims, persons with disabilities, or those in low-bandwidth regions who are nonetheless frequent users of messaging apps and group chats are not left behind. Hybrid models that prioritize audio and pictorial tools as well as traditional community outreach are essential to prevent a digital resilience divide.

Conclusions

Digital tools offer a potentially transformative path to enhance and extend support to victims of terrorism. By prioritizing accessibility and low-connectivity design, we can reach those who are currently underserved, whether due to geography, disability, or social stigma. Co-designing these resources with victims presents an exciting opportunity to empower victims and survivors while improving practical resources and tools to support their recovery and resilience. Further considerations on victim-centered tool design follow these conclusions.

As this field evolves rapidly, we must distinguish between tools of varying risk and at different stages of development and scale. In general terms, victim-facing applications carry higher risks than those designed for others, as they interact directly with individual trauma. In addition, the risks of tools that draw on vetted information about medical advice or existing services are not the same as those that seek to use generative AI, and the risks of tools that maintain a human-in-the-loop are not the same as those that operate under more limited or without human supervision. Because victims' needs change over time, we must ensure that the risk profile of any digital tool is appropriate for the survivor's specific stage of recovery. A more detailed examination of the cross-cutting risks of tool development in this space concludes this report.

This research has identified a few high-impact tools that are already operating at scale and could be adapted for victims of terrorism. These include mindfulness apps, multilingual service directories, and digital registration systems. By leveraging these technologies, we can help victims navigate their recovery with greater agency while using improved content moderation to protect communities from the trauma of viral disinformation and attack footage. In addition, AI-powered support for clinicians and VR-based trauma training for first responders show great promise. By testing and iterating these tools in collaboration with the victim community, we could develop scalable solutions that improve care and support worldwide.

Some areas of digital support, while conceptually powerful, remain at a lower level of technological or institutional readiness. These include the Digital Public Infrastructure that could underpin a seamless digital environment linking registration, support, and justice services, real-time data-sharing tools for incident response, and the use of blockchain and permissioned ledgers for evidence chain-of-custody and cross-border judicial cooperation. Currently, the ecosystem is siloed and experimental. Moving forward requires sustained investment to move through individual pilots and testing towards a more comprehensive, integrated digital support system.

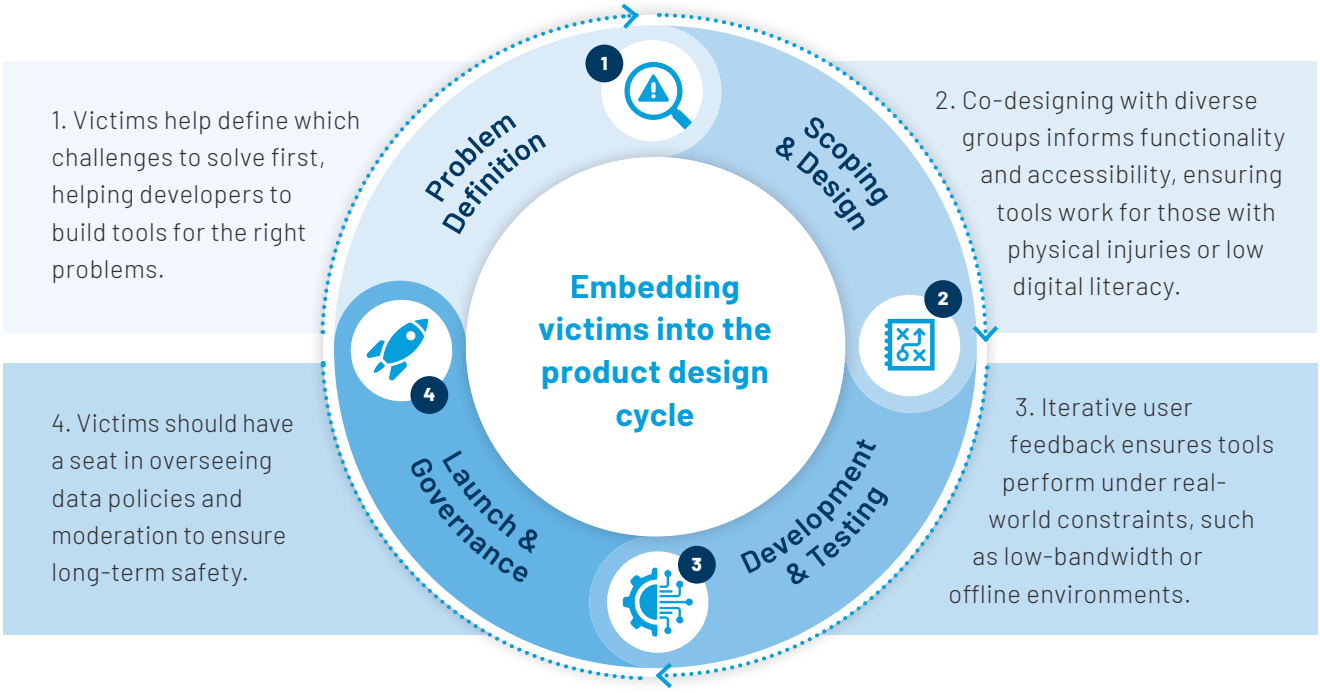
Considerations for victim-centered digital tool design

Involving victims and survivors in the design of digital tools is a prerequisite for success. Victims are "involuntary experts" in post-trauma needs; leveraging this expertise ensures that solutions are grounded in reality rather than assumptions. Furthermore, active participation helps restore the sense of agency often shattered by terrorism, making the design process itself a potential component of the recovery journey.

Community-centered digital design has matured from "user research and testing" toward co-design across the full lifecycle, especially in digital health and humanitarian tech. Industry standards increasingly treat end-user participation and feedback as non-negotiable, while newer guidance makes data responsibility and protection-by-design core to ethical deployment in crisis settings. In parallel, trauma-informed and victim-centric design is becoming a recognized specialization, reflecting that for vulnerable users, whether a tool 'works' or not can be a bigger question than just assessing functionality: tools must be assessed against their safety, privacy, and control of risks such as retraumatization, misuse or exfiltration of sensitive data, and raising unrealistic expectations in the results of using a tool. Across product design and adjacent applied research, there is a spectrum of approaches:

- **User-centered design:** users inform requirements and usability testing, but designers retain most decision power.
- **Participatory design / co-design:** users (or community representatives) are active collaborators through discovery, ideation, prototyping, and evaluation, often with shared decision-making.
- **Community-led design / Human Centered Design:** explicitly centers power in the hands of the most affected groups. This approach addresses power imbalances regarding data ownership, consent, and moderation policies, ensuring that marginalized subgroups are not excluded by linguistic or cultural barriers.

Engagement should not be a "one-off" event but a continuous integration across the development stages:



By embedding victims across the entire development cycle, we ensure that whether a tool is designed for the first hour of a crisis or for the tenth year of a judicial proceeding, it remains grounded in the expertise and agency of those it is built to serve. This level of engagement provides the necessary framework to address the reality that victim needs are not static but evolve across a distinct timeline of recovery. The tools we build must respect this progression from crisis "surge support" to service referral and sustainable MHPSS support, toward long-term advocacy, commemoration, and justice.

Existing standards and guidance, particularly from the humanitarian action space, frame participation, accountability, community feedback, and complaints mechanisms as core components of emergency preparedness and response. Examples include UNHCR's Accountability to Affected People guidance,[105] the United Nations Office for the Coordination of Humanitarian Affairs (OCHA)'s flagship initiative on participatory action,[106] and the Humanitarian Standards Partnership's Core standard.[107]

Data responsibility has also become core to the development and design of humanitarian and peace tech, with specific guidance on co-creating digital tools with crisis-affected people issued by CLEAR Global and the UK Humanitarian Innovation Hub,[108] OCHA's Data Responsibility Guidelines,[109] UNHCR's guide on designing safe digital MHPSS tools for displaced and stateless adolescents,[110] and Inter-Agency Standing Committee (IASC) operational guidance on data responsibility in humanitarian action.[111]

Co-design in fragile settings commonly uses low-fidelity prototypes such as simple mock-ups and wireframes, scenario-based testing, and ways of learning what you need from people without requiring them to re-live, disclose, or document sensitive experiences, and without putting them at social, legal, or physical risk. Guidance increasingly emphasizes trust-building and inclusion of those with the least power or voice.[112]

Outside of the humanitarian sphere, some work has been done on adapting trauma-informed approaches to technology more generally, recognizing that digital technologies can both cause and exacerbate trauma, and seeking ways to avoid technology-related trauma and retraumatization. Examples include adaptations of the US Substance Abuse and Mental Health Services Administration (SAMHSA) principles of trauma-informed care —safety, trust, collaboration, peer support, enablement, and intersectionality—to the design, development, deployment, and evaluation of computing systems.[113] A review of efforts to co-produce digital mental health interventions looked at different methodologies found that including end-users in the design improved cultural sensitivity and enriched the ideas developed.[114]

However, there are still some potential pitfalls that will need to be considered by digital tool developers when working with victims of terrorism.

For example, consulting users does not necessarily mean handing power to them. Many projects still invite feedback late, with little budget or time for victim advisors or for user-led steering groups. This keeps decision-making with implementers instead of affected people. Participation can be extractive if benefits, compensation, and decision rights are unclear.

105 https://emergency.unhcr.org/protection/protection-principles/accountability-affected-people-aap

106 https://www.unocha.org/flagship-initiative

107 https://handbook.hspstandards.org/en/chs/2024/

108 https://clearglobal.org/resources/human-centred-technology-design-in-humanitarian-action/

109 https://data.humdata.org/dataset/2048a947-5714-4220-905b-e662cbcd14c8/resource/8bc5b848-8ece-4f1f-a78b-18dd972bb21a/download/data-responsibility-guidelines-2025.pdf

110 https://www.unhcr.org/innovation/wp-content/uploads/2023/03/Designing-Safe-Digital-Mental-Health-and-Psychosocial-Support-MHPSS.pdf

111 https://emergency.unhcr.org/sites/default/files/2023-11/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action%2C%202023.pdf

112 https://clearglobal.org/resources/human-centred-technology-design-in-humanitarian-action/https://clearglobal.org/resources/human-centred-technology-design-in-humanitarian-action/, https://www.unicef.org/innovation/hcd

113 https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517475

114 https://pmc.ncbi.nlm.nih.gov/articles/PMC11044797/

Identifying and working with a diverse sample of intended users is also a challenge, as well as acknowledging the diversity of the needs and preferences of user groups and overcoming group dynamics of focus groups that may make some participants less likely to engage fully. Dialects, low-literacy interfaces, and audio or pictorial options are often under-resourced, which quietly excludes many intended users and participants from tool design.

Finally, clear and transparent communication and expectation management are vital to any successful co-design process. It must be clear to participating victims and communities where a tool is in its development journey to avoid misunderstandings about the likelihood and speed with which their engagement in design discussions will result in them being able to access and share a 'real' tool at scale. Many concepts do not become pilots, and many pilots do not scale. Ensuring that there is clarity from the beginning can avoid or mitigate the risks of frustration later down the line.

Common risks and limitations

Unlocking the promise of digital innovation for victims of terrorism depends on a clear-eyed assessment of cross-cutting risks. Digital tools are not a "one-size-fits-all" solution; their safety and efficacy depend on their design, their intended users, and the sensitivity of the data they handle. To adhere to the principle of "Do No Harm," a proactive, risk-based approach must be integrated into every stage of the development lifecycle.

The level of risk associated with a digital tool is not static. It is determined by several critical factors that must be evaluated before deployment:

- **User Proximity:** Victim-facing tools carry significantly higher risks than those designed for clinicians or service providers, as they interact directly with individual trauma and vulnerability.
- **Information Integrity:** Tools that draw on a vetted, established corpus of information (such as service directories) have a different risk profile than those utilizing generative AI, which may produce unpredictable or "hallucinated" outputs.
- **Human Oversight:** The presence of a "Human -in-the-Loop" remains a primary safeguard. Tools operating with limited or no human supervision require more rigorous technical and ethical guardrails and may not be appropriate for sensitive use cases.
- **Temporal Sensitivity:** Victim needs and vulnerabilities shift over time. A tool that is helpful during long-term advocacy may be inappropriate or even harmful during the acute "surge" phase following an attack.

While specific tools require tailored management, several common considerations apply to all digital interventions in this space. The following sections explore these cross-cutting risks, providing a foundation for safe, responsible, and victim-centered innovation.

Human rights and gender considerations

- **Digital services can unintentionally amplify existing inequalities, particularly if gender, linguistic and cultural diversity, and accessibility features are not built in from the start:** Involving victims of terrorism in design and testing is a major step, but it is not sufficient if participation is dominated by communities that are already better connected, more visible, or more able to engage in international processes. Without deliberate inclusion of men, women, and youth of varied abilities, languages, dialects, and cultural contexts, benefits may skew toward those with the most capacity to participate rather than those with the greatest need.
- **Safety, privacy, and trust are foundational, and become more complex as systems incorporate AI:** Platforms that store or process sensitive victim data must meet an extremely high bar for protection and accountability. The risks are not only technical (data breaches, insecure integrations, malicious attacks), but also social (coercion, intimidation, misinformation, and manipulation). Failures could put victims' lives, as well as their well-being, at risk.

- **Greater connectivity comes with greater exposure:** Digital spaces that connect victims can be powerful sources of solidarity, but without strong safeguards they can also expose users to harassment, doxxing, or targeted abuse, potentially worsening harm instead of reducing it.
- **Safeguards should be built in from the beginning, not bolted on later:** In practice, this means collecting only the data that is absolutely necessary, limiting who can access it, and designing data architecture with the assumption that systems may be targeted or misused. It also means being clear in advance about "red lines" and the kinds of sensitive cases where automated responses are inappropriate and a human-led pathway is required.
- **Even trauma-informed tools can cause harm:** Victims of terrorism have specific needs and vulnerabilities. Great care must be taken to minimize potentially unwanted push notifications about attacks, restrict algorithmic amplification of attack-related content, and understand the emotional burden for users of maintaining a presence on a platform that may surface painful memories. Many tools are designed with sustained engagement as a core metric for their success but features that promote a tool's use should not come at the expense of the well-being of the user.
- **Children and youth have specific risk profiles that need accounting for:** Emerging research on sustained interactions between young people and AI chatbots and companions has raised important questions about potential negative impacts to their mental health and psychosocial development. Extra care needs to be taken when designing tools for young audiences, or tools that could be accessed by young users.
- **Not all victims and service providers will turn to trauma-informed tools for assistance:** Even if trauma-informed tools are developed and available at scale, not all victims and service providers will use them. They may develop their own tools, procure from different providers, or turn to freely available platforms that have fewer guard-rails in place. Continued engagement with the tech sector is essential to ensure that "victim-centric" design becomes an industry standard, not just a feature of specialized apps.

Accessibility and sustainability

- **Tools must be accessible-by-design:** Many victims of terrorism suffer life-changing injuries, ongoing trauma, and other challenges that can change the way they are able to interact with digital tools and services. Building with these challenges in mind is essential to ensuring that tools are equipped to best support these communities.
- **Human support must remain central:** Automated screening or triage can help manage volume and speed up referrals, but it should always be paired with clear handoffs to trusted local actors. Victims should be able to reach a person when needed, and communities should have up-to-date, offline-aware "service maps" so that referrals still work when systems fail or connectivity drops.
- **Cost can limit access:** Subscription models, paid platforms, and short-term pilots can create inequity and discontinuity, particularly for communities already facing economic strain or unstable access to services. For many victim populations, continuity of services may require public investment, philanthropic backing, or blended financing models that can maintain essential services over time.
- **Choices about openness and interoperability matter:** Solutions built as closed, proprietary systems can limit collaboration, complicate cross-border use, and restrict future adaptation. Vendor lock-in may reduce flexibility just when evolving needs and new partnerships require systems to be extended, integrated, or repurposed.
- **Barriers to implementation are not just technical:** National platforms and coordinated systems can be transformative, but they require cross-ministerial alignment, clear governance over content and data, ongoing localization, and sustained operational capacity, conditions that may be difficult to maintain in fragile or crisis-affected contexts.

- **There is a risk of "quality drift" and over-reliance:** If digital tools are treated as substitutes for in-person care rather than complements, they may normalize low-intensity support even when clinical intervention is needed. Clear boundaries and communication matter to ensure that users and providers understand what a tool can and cannot do, when additional help is necessary, and how to access it.
- **Measurement matters:** Metrics for the success of commercial digital tools are well-established, but do not translate well to social impact innovation. While some tools in this space may be commercially viable and income-generating for their developers, other metrics for success will need to be developed to evaluate the impact of digital tools on victim outcomes over time, including metrics such as time-to-service, user retention, and qualitative indicators of victim wellbeing and empowerment. In addition, evaluation methodologies for assessing the trauma-informed capabilities or victim-centricity of existing tools are also currently lacking and will require further work.

Additional considerations for low-connectivity and resource-constrained settings

- **Tools need to be grounded in local realities:** Solutions should draw on evidence-based, scalable approaches that support the realities of post-crisis care in difficult contexts, while monitoring impact carefully and adapting based on real-world learning. For example, in the MHPSS space, this may lead to a greater emphasis on building tools that help non-specialists to deliver safe, structured assistance rather than assuming a large user-base of trained clinical specialists.
- **Low bandwidth is a feature, not a bug:** This typically means prioritizing channels that work on basic phones (for example hotlines, SMS, and USSD) and ensuring services remain usable even when connectivity is intermittent. Where apps or web tools are appropriate, content can be designed to load gradually, work offline where possible, and avoid unnecessary data use. Not every promising new feature improves victim care outcomes and can instead add complexity or load times on poor connections.
- **Language and literacy are essential design requirements:** Many users will need voice options and local language coverage, and some will benefit more from audio or pictorial guidance than text-heavy interfaces. Tools should anticipate code-switching, dialect variation, and the realities of how people communicate in crisis.
- **Under-representation of low-connectivity communities has a knock-on effect on the performance of AI-based solutions:** As well as structural barriers such as poor access to the internet and intermittent energy, 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 tools' ability to serve these populations. Translation and linguistic ability are one problem-set, but cultural fluency including the understanding of how bias, discrimination, trauma, and mental health cues are expressed in diverse cultural contexts is another. While acknowledging the important efforts of a number of organizations and initiatives to bridge this gap, more work is still needed in this space to ensure that this important digital divide is bridged, not widened.

Recommendations

Harnessing the opportunities and addressing the risks presented by new technologies will require a genuinely multi-sectoral effort. The United Nations, governments, industry, academia, civil society, victims, and victims' associations each have an important role to play in ensuring that digital innovation is safe, inclusive, and responsive to the needs of victims of terrorism.

In this context, UNOCT stands ready to support Member States in strengthening victim-centered approaches and improving the support available to victims of terrorism, while also convening and partnering with the private sector and academia to align new technologies and victim needs to find innovative solutions to hard problems.

Opportunities for governments

- **Digitize victim response:** Effective crisis support depends on accurate, up-to-date information on who has been affected and what services are available. This information needs to be coordinated across ministries and kept current to enable rapid use in emergencies. Allowing international and non-governmental actors to contribute to service mapping can also improve reach, while integrating crisis response and justice-readiness into Digital Public Infrastructure roadmaps can help future-proof these efforts.
- **Create a "no wrong door" system:** Victims should be able to digitally register once for support, through whichever ministry or agency they first encounter. Governments should develop secure systems to manage and share this information across relevant entities, reducing the burden on affected individuals to repeatedly prove their eligibility.
- **Invest in next-generation training:** VR and AI-driven victim avatars can help digitize crisis training for police, medical personnel, and other first responders. These tools offer a scalable and cost-effective way to practice trauma-informed engagement. Governments should work with the private sector to develop context-appropriate tools and support access for countries that may not be able to build such systems independently.
- **Bridge the digital divide:** Digital support should be designed to reach those most at risk of exclusion, including older survivors, youth, women, persons with disabilities, and individuals in low-bandwidth settings. Governments should fund hybrid models that combine high-tech tools with low-tech and accessibility-by-design approaches, while also investing in AI research and partnerships that improve the representation of local cultures and languages in digital systems.

- **Strengthen data governance and accountability:** Sensitive victim data requires robust protection. Governments should work with the private sector to implement strong security protocols, privacy-by-design safeguards, and clear accountability frameworks, including audit mechanisms to address situations where digital tools or systems result in inadvertent harm or data breaches.

Opportunities for industry and academia

- **Invest in social-impact technology:** Supporting victims of terrorism requires sustained investment in digital tools designed for social impact. Investing in social impact technology is not merely a philanthropic gesture, it drives technical breakthroughs, builds public trust, and helps humanity solve for its hardest problems. This may require some mindset shifts from commercial models of product development. For example, features that maximize user engagement in other contexts may be harmful in trauma-related settings, where repeated exposure to distressing content can deepen harm.
- **Make co-design an industry standard:** The private sector and academia should work with victims and survivor communities to move beyond consultation toward genuine co-design. Survivors should be involved throughout the lifecycle of a tool, from problem definition and scoping to testing, evaluation, and governance, to ensure that solutions respond to real needs.
- **Boost research into multicultural AI:** More research and pilots are needed to develop AI models that can handle cultural nuance and sensitive cues effectively. Multicultural AI is especially important when developing tools for users experiencing grief and trauma, where cultural nuance shapes user needs and responses in ways that cannot be solved through translation alone.
- **Consider "crisis mode" protocols for general-purpose AI:** In the aftermath of high-stakes events like terrorist attacks, solutions are needed to identify and address AI-generated disinformation that targets victims, including fabricated images or other deceptive content designed to cause further harm. Private sector platforms have a significant role to play in creating a safer online environment for victims of terrorism.
- **Build safe hand-off mechanisms:** General-purpose platforms should develop automated, trauma-informed pathways that direct users seeking support toward specialized and professional mental health and psychosocial services. These hand-off mechanisms can help ensure that users are not left relying on tools that are not equipped to meet their needs, which is particularly important for young users and vulnerable individuals.

There are many talented individuals and organizations working on solutions that can make the storage of sensitive victim information safer, more robust, and easier to implement even in resource-constrained settings. Similarly, many individuals and organizations have a huge amount of expertise in designing for low-connectivity, low-literacy, and crisis-affected contexts. By comparing experiences, exchanging best practices, and investing in shared understandings, we can improve support to the individuals and communities affected by terrorism worldwide.

To end this report with a common refrain from members of the Victims of Terrorism Associations Network (VoTAN):

> ***"If you want to go fast, go alone.***
> ***If you want to go far, go together."***

Looking Ahead

The opportunity now is to translate this growing body of research and innovation into practical, rights-respecting support that reaches victims of terrorism worldwide. This calls for sustained dialogue on how to co-design, develop, and adapt digital tools, building from existing services and proven approaches, rather than starting from scratch. Above all, it requires greater collaboration between governments, academia, the private sector, and international organizations to align standards, share learning, accelerate research, and invest in solutions that are inclusive, secure, and sustainable so that digital innovation genuinely advances the rights and supports the needs of victims of terrorism.

Following the launch of this Gap Analysis of Digital Tools to Support Victims of Terrorism in April 2026, UNOCT will establish a series of practitioner working groups that bring victims, industry, academia, international organizations, and other stakeholders together to translate these findings into a roadmap of priority innovation areas and pathways for victim-centered digital tool design, to be launched as a Toolkit for Technology-Enabled Support for Victims of Terrorism.

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre (UNCCT)