

Centring Victims in Global Cyber Norms implementation:

Embedding the Harm Methodology in
the UN's Regular Institutional Dialogue

Table of Contents

Executive Summary	3
<i>What is a victim-centric approach?</i>	3
<i>Why does it matter now?</i>	3
<i>Key recommendations at a glance</i>	3
Cross-cutting	3
DTG-specific	4
<i>What we hope happens next</i>	4
Introduction	5
Implementation gaps	6
Landscape review: OEWG and the Global Mechanism	8
Recommendations: Embedding a Victim-Centric Approach in the Global Mechanism	11
<i>Cross-cutting recommendations</i>	11
<i>DTG-specific recommendations</i>	12
DTG 1: Specific challenges in ICT security across all five framework pillars	12
DTG 2: Cyber Capacity Building	12
Conclusion: A Call to Action	14
Appendix: Harm Methodology	15

Acknowledgements

This paper was authored by Daniela Schnidrig and Sheetal Kumar for the CyberPeace Institute.

Executive summary

This paper argues that the implementation of the UN framework for responsible state behaviour in cyberspace can be significantly strengthened by embedding a victim-centric approach, particularly within the new Global Mechanism and its Dedicated Thematic Groups (DTGs). A victim-centric approach shifts focuses on real-world human, societal and systemic impacts of cyber operations, and can support more effective, inclusive, and resilient cyber governance.

What is a victim-centric approach?

A victim-centric approach places the experiences and needs of affected populations at the centre of cyber policy and decision-making. It emphasises systematic harm documentation, inclusion of survivor voices, and evidence-based policy responses. The [Harm Methodology](#), developed by the CyberPeace Institute, provides a flexible and actionable framework which can be applied to a wide range of contexts to assess the multidimensional impacts of cyber incidents, supporting data-driven implementation of norms, CBMs, international law, and capacity building.

Why does it matter now?

With the OEWG's final report adopted and the establishment of the Global Mechanism as a permanent forum in March 2026, we have an opportunity to build on existing agreements relating to responsible state behaviour in cyberspace and ensure an evidence-based approach to implementing agreed commitments and addressing commonly agreed threats. Integrating victim-centric approaches at the Global Mechanism can ensure that the new mechanism supports not only national security and geopolitical dialogue, but also the lived realities of harm and recovery for individuals and communities, organisations and institutions affected by cyber threats.

Key recommendations at a glance

Cross-cutting

- Institutionalise victim-centric thinking in DTG agendas and discussions.
- Ensure meaningful and inclusive stakeholder participation, including non-ECOSOC actors.
- Create a standing agenda item in plenary focused on harm and resilience.

- Encourage case study sharing and use of Harm Methodology as a common framework.
- Promote multistakeholder dialogue with technical, humanitarian, academic and CSO inputs.

DTG-specific

- **DTG 1:** Use thematic discussions (e.g. ransomware, critical infrastructure attacks) to assess harm and integrate relevant norms, legal perspectives, and resilience practices including in line with emerging threats such as artificial intelligence.
- **DTG 2:** Tailor capacity building activities to support harm reduction, victim engagement, and response coordination, drawing on multistakeholder partnerships.

What we hope happens next

We encourage States to embed these approaches into the Global Mechanism's early planning, especially in the framing of DTG agendas. We also encourage civil society, academia, and technical experts to align their contributions with these priorities to maximise their impact.

Introduction

Over the past decade, the international framework for responsible state behaviour in the use of ICTs has advanced significantly, establishing norms, capacity building frameworks, and confidence-building measures through consensus-based processes at the United Nations, including the Open-Ended Working Group on ICTs (OEWG). Yet, practical implementation remains limited and uneven across contexts, and States and stakeholders have consistently emphasised the need for more contextualised, actionable guidance to support implementation.

One major reason for this gap is that cyber norm implementation has largely remained focused on threats and national security imperatives rather than the real world impacts on people and communities. As a result, the harms experienced by individuals - especially civilians affected by cyber operations targeting healthcare, humanitarian services, or critical infrastructure - remain underexamined and underaddressed.

Yet, a victim-centric approach to cybersecurity has begun to gain traction. This approach focuses on the experiences and needs of affected populations, recognising that cyber operations often cause cascading harms. The Harm methodology, developed by the CyberPeace Institute, provides a framework to systematically map and categorise these harms across human, institutional, economic, and informational domains.

Integrating this lens into cyber norms implementation can help:

- Strengthen resilience to systemic and emerging threats, including artificial intelligence;
- Provide a basis for measuring norm adherence and policy impact, notwithstanding technological changes;
- Enable more inclusive and legitimate decision-making processes.

As the international community moves towards operationalising the new Global Mechanism, there is a critical opportunity to embed this approach from the start.

Implementation gaps

Our research identifies four interrelated categories of gaps that prevent the operationalisation of a victim-centric approach. These not only impede harm mitigation, but also weaken the effectiveness, legitimacy, and resilience of cyber norms implementation more broadly.

1. Data and evidence gaps

- There is no accepted framework for the collection, sharing and management of cyber harm data. This includes uncertainty around what types of harms should be documented, what indicators should be used, and how data should be stored or anonymised.
- Victims and civil society lack access to relevant data, either due to classification, institutional silos, or political sensitivities.
- Incident analysis remains politicised, undermining neutrality and impeding evidence-based policy responses.

How a victim-centric approach helps:

- Establishes clear typologies, indicators, and tools for assessing harm across contexts; promotes open-source, anonymised harm tracking to support transparency.

2. Structural and governance barriers

- Cross-sectoral information sharing, particularly between public, private and humanitarian actors is poorly developed and often ad hoc.
- States differ significantly in their governance systems, technical capacity, and political willingness to prioritise harm mitigation.
- Cultural and legal divergences complicate consensus around what constitutes “harm” or what kind of harm matters.

How a victim-centric approach helps:

- Promotes inclusive coordination across governments, humanitarian actors, and CSOs; supports context-sensitive governance practices.

3. Methodological limitations

- Existing tools, like the Harm Methodology, require further development, especially around quantification, indicator design, and integration into policy frameworks.
- Few illustrative case studies exist to demonstrate the real-world application of victim-centric models, particularly in multilateral or national cybersecurity settings.

How a victim-centric approach helps:

- The Harm Methodology offers a structured, adaptable tool for mapping harm, and can be piloted through multilateral or national initiatives.

4. Stakeholder exclusion

- Key actors with harm-related experience, such as humanitarian responders, public health experts, and victim advocates are underrepresented in cyber norms dialogues.
- Victim communities and researchers remain largely excluded from institutional decisionmaking at the UN level, undermining both the inclusivity and relevance of current mechanisms.

How a victim-centric approach helps:

- Provides an entry point for including lived experience and localised expertise; enhances legitimacy of international processes.

Landscape review: OEWG and the Global Mechanism

The final report of the Open-Ended Working Group (OEWG) on ICTs, reflected in document A/AC.292/2025/CRP.1, marks an important step toward operationalising the framework for responsible state behaviour in cyberspace. This section analyses the OEWG report through the lens of a victim-centric approach, as advanced by the CyberPeace Institute's Harm methodology, and assesses the extent to which the report (including the structure of the new Global Mechanism and its Dedicated Thematic Groups (DTGs), supports such a perspective).

Substantive recognition of victim harm

The report contains multiple references to the impact of malicious ICT activity on **civilians, humanitarian actors, and critical infrastructure**. For example, States acknowledge the increased use of ICTs in conflict, and the potential for these tools to affect civilians and civilian objects (para 15), including humanitarian operations (para 21). Furthermore, it identifies the indirect and direct harms caused by covert information operations, including **societal destabilisation** (para 22), the **cascading effects** of ICT attacks on critical infrastructure (paras 17, 34), and that they can pose direct and indirect harm to **individuals** (para 22).

While these references demonstrate a growing awareness of the human consequences of cyber threats, they tend to frame harm primarily in terms of geopolitical or operational risks rather than centering the experience and needs of affected populations. Notably absent is a systematic approach to understanding, measuring, and responding to the multi-layered harms experienced by victims. The report's narrative remains largely State-centric and national security-focused, rather than people-centric and resilience-driven.

Operational threats and critical infrastructure: recognising the human impact

One of the clearest avenues through which the OEWG report touches on a victim-centric approach is its treatment of threats to critical infrastructure (CI) and critical information infrastructure (CII). The report dedicates significant attention to threats such as ransomware, wiper malware, and other malicious software, acknowledging their capacity to disrupt essential public services and generate cascading harms across borders (paras 17, 24, 34).

While these sections are framed in technical and political terms, they implicitly point to the human consequences of cyber operations. For instance, ransomware attacks targeting hospitals, energy systems, and municipal services can directly affect individuals' access to healthcare, safety, and livelihood. The report recognises that such threats “pose an elevated risk of harm to the population and can be escalatory” (para 34), thereby aligning with core tenets of a victim-centric approach, even if not explicitly articulated as such.

Moreover, the acknowledgement of cross-border cascading effects from CI - CII disruptions (para 17) suggests a systematic understanding of harm that aligns with the Harm Methodology's emphasis on interdependent impacts. In this regard, the OEWG text creates an opening for more structured efforts to measure, map, and mitigate harm to populations, particularly through data driven analysis and inclusive risk assessments.

Emerging entry points: The role of CCB and trust

Cybersecurity capacity building (CCB) is framed in the report as a cross-cutting and foundational element of the OEWG's work (paras 8-9). This presents a meaningful entry point for embedding a victim-centric perspective. For example, language around developing “resources, skills, policies and institutions” to increase ICT resilience (para 9) is directly relevant to mitigating harm to populations. The emphasis on inclusive partnerships and multistakeholder cooperation - including civil society, humanitarian organisations, and academia - (para 53 k), offers further room to integrate victim-centric models of threat detection, response and recovery.

The current framing of CCB does not explicitly include support for harm documentation, victim redress, or data collection and sharing; areas where the Harm Methodology could provide a clear, structured contribution.

The Global Mechanism and DTGs: A platform for institutionalising a victim-centric approach

The Global Mechanism and its two Dedicated Thematic Groups (DTGs) provide concrete platforms for advancing the harms-based approach:

- DTG 1, which will address “specific challenges” in ICT security across all five framework pillars, offers space to explore and integrate harm measurement tools into international cyber norms implementation.

- DTG 2, focusing on capacity building, is especially suited to operationalising victim-centric strategies, supporting training, partnerships, and methodologies to quantify and respond to victim harm.

Importantly, both DTGs are expected to include stakeholders such as technical experts, civil society, and academia. Their design - including structured discussions on lessons learned, guiding questions, and action-oriented recommendations - could be leveraged to ensure systematic attention to harm mapping, disaggregated data on affected populations, and best practices.

Gaps and missed opportunities

While the OEWG's final report shows increased awareness of the real-world impacts of malicious ICT activity, it falls short of embedding a victim-centric approach. Key missed opportunities are evident in both the substantive and procedural dimensions of the report.

Substantively, the report does not institutionalise mechanisms for documenting or addressing victim harm - such as ethical data collection, support for survivors, or the inclusion of civil society actors with direct experience of affected populations.

A notable gap, especially given its resonance during OEWG deliberations, is the exclusion of language drawn from the International Committee of the Red Cross (ICRC) and its work on ICTs in armed conflict. Throughout the OEWG sessions in New York, a number of States expressed strong support for integrating references to the ICRC's resolution and its emphasis on humanitarian protections in cyberspace. This resolution would have provided a credible normative anchor for incorporating victim-centric language, yet was ultimately not reflected in the final report.

Procedurally, although the OEWG promotes multistakeholder participation, the non-objection mechanisms remain a potential barrier to the inclusion of civil society, including victim-oriented organisations and affected community voices. In practice, this may result in the systematic exclusion of actors critical to harm assessment and victim support - undermining the promise of an inclusive Global Mechanism.

Recommendations: Embedding a Victim-Centric Approach in the Global Mechanism

As the Global Mechanism and its DTGs take up the mantle of implementing the framework for responsible State behaviour in cyberspace, it is essential that victim centricity is embedded not only as a value, but as a practical methodology. The following recommendations outline how the Global Mechanism and its DTGs can both be strengthened by and serve to advance a victim-centric approach.

Cross-cutting recommendations

- **Institutionalise victim-centric thinking:** ensure DTG meetings include consideration of human impact, including disaggregated harm, social vulnerability, and resilience. Employ the Harm Methodology as a framework.
- **Ensure meaningful engagement of stakeholders:** encourage and resource participation from affected communities (e.g those who have lived experience of attacks on critical infrastructure) and harm-focused civil society groups, including those without ECOSOC status.
- **Standing harm agenda in plenary:** establish a recurring agenda item in the Global Mechanism plenary focused on lessons learned from past incidents, including harm mitigation practices.
- **Share national and regional experiences:** encourage States to submit case studies, examples, and national practices related to harm documentation, response, or survivor support. Employ the Harm Methodology as a common analytical framework.
- **Multistakeholder dialogue facilitation:** design DTG formats to enable interaction between government, civil society, humanitarian actors, technical experts, and academia, with a focus on shared challenges and localised harm response.

DGT-specific recommendations

DTG 1: Specific challenges in ICT security across all five framework pillars

- Identify and ground discussions on specific challenges and threats, building on agreed language (e.g. those included in the OEWG CFR), and encourage states to focus their discussion to address the cross-cutting nature of each challenge (e.g. how it relates to the norms and to their international law positions and how artificial intelligence (AI) technologies amplify or mitigate these challenges). For example:
 - **Cyberattacks on critical infrastructure:** share national experiences on the use of malicious software, threat vectors, and the resulting harms using the Harm Methodology. Reference discussions in other relevant regional or multilateral forums. Discuss the challenges and opportunities presented by AI, including the types of data needed to assess them.
 - **Ransomware:** discuss the frequency, scale, and severity of harm caused by ransomware, linking these to relevant norms (e.g. norm i) and international law, and the impact of AI on ransomware operations.
 - **Commercially available ICT intrusion capabilities:** share understandings of the malicious use of such tools, including their impact on human rights and victims, as well as the impact of AI on these capabilities
 - **Incident response and recovery:** share practices for effective incident response, including challenges such as trust deficits and lack of interoperable data standards. Highlight mechanisms that demonstrably reduce harm.

DTG 2: Cyber Capacity Building

- Integrate and synchronise capacity building discussions with DTG 1, for example:
 - **Cyberattacks on critical infrastructure:** advance discussions on cyber resilience and engage humanitarian/technical responders to support norm implementation (e.g. norms f, g, h).

- **Ransomware:** build evidence-based understanding of harm caused and share initiatives to counter the threat, referencing existing multilateral and regional efforts. Identify how capacity to protect critical infrastructure (e.g. in detection and mitigation) needs to evolve to address emerging threats, including from agentic and generative AI.
- **Commercially available ICT intrusion capabilities:** present commitments and initiatives to address misuse; include briefings from victims.
- **Incident response and recovery:** share good practices on norm implementation (e.g. norm k), especially multistakeholder collaboration (e.g. CERTs, law enforcement, civil society). Identify areas where emerging threats require data collection to advance capacity building efforts for all stakeholders.

Conclusion: A Call to Action

The Global Mechanism represents a turning point for the international community's approach to responsible state behaviour in cyberspace. It offers the chance to move from consensus on principles to meaningful implementation.

Embedding a victim-centric lens at this early stage is essential to ensuring the mechanism delivers not only on political dialogue, but also on the ground realities of harm, resilience, and recovery. Doing so will help make the mechanism more legitimate, evidence-based, and responsive to the needs of those most affected by cyber threats.

We encourage States and the broader stakeholder community to take up this opportunity to adopt inclusive modalities, centre human impact, and work collaboratively to protect populations.

Appendix: Harm Methodology

Introduction and Purpose

The Harm Methodology is a standardised framework initiated by the CyberPeace Institute in 2022 to understand, track, and measure the human and societal costs resulting from cyberattacks. Its primary strategic objective is to identify methods for assessing the harm of a single cyber incident across multiple indicators and distinct categories of harm. Ultimately, the methodology is designed to provide a human-centric, evidence-based tool to help States build stronger accountability measures and enforce responsible behavior in cyberspace.

Context and Rationale

While the frequency, scope, and severity of cyberattacks have increased at an alarming pace, the traditional frameworks used to measure their consequences have remained limited. Current assessments predominantly focus on the direct operational or financial impacts on targeted organisations, measuring factors such as system restoration time, financial costs, and the number of breached records.

This narrow assessment fails to capture a fundamental element: the actual harm that cyberattacks cause to people and society. Because there has historically been no standard methodology to estimate these broader societal impacts, the resulting lack of evidence impedes effective policy-making, resource allocation, resilience efforts, and the pursuit of accountability for victims. The Harm Methodology aims to fill this critical gap.

Core Components and Research Basis

The methodology is built upon research into specific categories and indicators of harm, notably including physical and psychological harm. The framework leverages data analysis and case studies, specifically drawing upon:

- Repositories and analyses of cyberattacks against the healthcare sector tracked between June 2020 and September 2022.
- Repositories and analyses of cyberattacks against the civilian population within the context of the conflict in Ukraine between January 2022 and December 2023.
- Case studies that map available data to specific indicators of harm.

Strategic Value and Policy Application

The Harm Methodology serves as a practical, data-driven tool for policy and decision-makers working to advance international peace and security. It directly supports the implementation of the UN framework for responsible State behaviour in cyberspace. Specifically, it assists States in fulfilling recommendations to transparently classify Information and Communications Technology (ICT) incidents based on their scale, seriousness, and impact on critical infrastructure.

Furthermore, the methodology strengthens the capacity to design evidence-based recommendations that inform multilateral negotiations, such as those conducted by the UN Open-Ended Working Group (OEWG) on security in the use of ICTs.

