CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

CyberPeace Institute's Statement

for the seventh session of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

Advancing the framework of responsible State behaviour in cyberspace through the Harms Methodology

In anticipation of the seventh substantive session of the UN Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG), the CyberPeace Institute[1] welcomes the opportunity to submit a statement outlining how a standardised methodology measuring harm from cyber incidents can contribute to inform the OEWG work and advance operationalisation of cyber norms. This submission builds on the Institute's established work to advance human-centric views on responsible behaviour in cyberspace particularly on the protection of humanitarian NGOs[2] and critical infrastructure,[3] as well as in developing the Harms Methodology[4] to measure the harms and impacts of cyberattacks and incidents.

The need for evidence-based accountability

Over the past few years, cyberattacks and operations against critical infrastructure have expanded in frequency, scale, sophistication, and severity. These incidents have very real consequences: they cause the destruction of systems and data, disrupt essential services, facilitate data theft and leak, and limit access to accurate information that can exert adverse and compounding effects on the daily lives of people. Any measures seeking to advance responsible behaviour in cyberspace

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

meaningfully and holistically must be, therefore, based on the recognition that cyberattacks and incidents do not just attack or harm technology, do not always have (easily) reversible effects, and can have impacts at national and international levels.

The CyberPeace Institute has been employing its analytical capacity of cyberattacks and incidents[5] against the healthcare sector and in relation to an armed conflict to map the impact of the malicious use of cyber on individuals and society. These data-driven platforms and analysis provide evidence of the increasing negative impacts and risks to vulnerable communities in cyberspace. However, the Institute also identified that the available metrics, tools, and frameworks do not provide for a standardised method to assess the harm of cyberattacks and incidents. This undermines a true evaluation of the scope and magnitude of such attacks, which further impedes policy making, resilience efforts and a means to affirm the real harm of a cyberattack or a cyber incident for victims, including in accountability processes.

A clarification on what constitutes harm in a comprehensive and measurable manner is thus required, coupled with data-driven and evidence-based metrics, tools, and frameworks for understanding, tracking, and measuring this harm.

Recognising this, the CyberPeace Institute initiated, in 2022, research and a process to develop a harms methodology, a standardised methodology to measure the harms and impacts of cyberattacks and incidents on people, society and the environment. The strategic objective is to determine and establish the means to measure harm from cyberattacks and incidents in order to increase knowledge of the human costs and influence policy, accountability, and resilience efforts.

Initial work on the Harms Methodology was presented at an expert meeting convened by the CyberPeace Institute in November 2023. The Report of the Expert Meeting on the development of a Harms Methodology[6], published in December 2023, provides a summary of the detailed observations and recommendations by the

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

representatives from across the diplomatic, policy, civil society, and academic communities, and independent experts, and how these are reflected in the ongoing work to develop the Methodology. This Report also serves as the basis for continued consultation of States, experts, and other stakeholders over the coming months to continue to develop and finalise the Methodology.

Advancing responsible behaviour through a data-driven harms methodology

A standardised data-driven harms methodology and metrics to understand, track, and measure the harm from cyberattacks and cyber incidents can serve to further advance transparency and predictability in operationalising existing norms, help track the implementation process, and enhance needs-driven approaches to identifying potential new norms of responsible behaviour of States in cyberspace.

As the OEWG seeks to advance the implementation of the agreed-upon framework, in the Second Annual Progress Report (APR), States agreed to elaborate additional guidance on the implementation of norms, including a checklist.[7] The Group further set out to explore specific areas in which the implementation of the agreed norms is currently lacking, or where existing implementation efforts can be improved. In this regard, the Harms Methodology could provide an important evidence-driven and human-centric guidance to be leveraged to accelerate these implementation efforts.

The persisting lack of shared understandings and clear definitions is a factor impeding operationalisation of cyber norms. The agreed-upon normative framework uses many different terms – often interchangeably – to explain the resulting consequences of a cyberattack or incident including “results”, “effects”, “impact”, “outcome”, “damage”, “implications”, “impairs”, and “harm”. Precise definitions with broad support are important for clarifying and demarcating the steps to norms implementation as well as for tracking and analysing conduct in cyberspace in order

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

to provide information on measures – their implementation and effectiveness – for responsible behaviour and accountability.

Explicating classifications for the impact and harms of cyber incidents is particularly relevant for the implementation of the following norms:

- *"a. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be* ***harmful*** *or that may pose* ***threats*** *to international peace and security; …*
- *b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the* ***consequences****; …*
- *f. A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally* ***damages*** *critical infrastructure or otherwise* ***impairs*** *the use and operation of critical infrastructure to provide services to the public; …*
- *i. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of* ***harmful*** *hidden functions; …*
- *k. States should not conduct or knowingly support activity to* ***harm*** *the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State… …".* [8]

A standardised harms methodology and metrics would further support the framework across other pillars, including confidence building measures. For example, its development and operationalisation are directly in line with the

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

recommended step in the Second APR encouraging States to share national views on technical ICT terms and terminologies to enhance transparency and understanding between States[9]. Increasing transparency about the terminology of the resulting consequences of a cyberattack or incident can contribute to greater predictability and enhance trust and confidence between and among States and contribute to advancing human-centric views in the operationalisation of the normative framework.

Needs-driven approach and targeted capacity building

States have agreed that implementing the normative framework requires targeted capacity building efforts. The multistakeholder community already informs and drives many such initiatives. For example, the UN Institute for Disarmament Research (UNIDIR) has provided a framework document[10] that elaborates the "Foundational Cyber Capabilities" relevant for States to implement the eleven norms of responsible behaviour. This includes:

- in relation to Norm B having a "Classification (public or non-public) of ICT incidents in terms of scale and impact"[11], and
- in relation to Norm F and G having a "Classification (public or non-public) of ICT incidents in terms of scale and seriousness"[12].

In this regard, the CyberPeace Institute's Harms Methodology can become an important capacity building tool made available to policymakers to contribute to evolving policy negotiations and to practitioners focused on building stronger accountability measures. This Methodology also aligns with agreed-upon principles on capacity building in relation to State use of ICTs in the context of international security[13], particularly the identified need for sustainable, evidence-based, transparent, and accountable measures that would include collaborative design.

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

The Second APR encourages States to develop and share tools that would assist States in incorporating a gender perspective into capacity-building efforts.[14] This is an important consideration as indiscriminate cyberattacks against parts of critical infrastructure can have differential impacts depending on the victim's gender identity. For instance, breaching the confidentiality of medical data can affect not only women's privacy but also their sexual and reproductive health rights, dignity, self-development, societal and psychological well-being, and physical security. As gender can be a factor impacting the severity of harms inflicted by cyber incidents, capacity building tools must inform strategies and policies to better address and eliminate gender-specific assaults in cyberspace, and to protect individuals who are disproportionately impacted due to their identity. The Expert Meeting on the development of a Harms Methodology organised by the CyberPeace Institute also highlighted that the Methodology should include considerations of gender-based violence.

The Second APR invites States to support capacity-building programmes in collaboration with stakeholders, including businesses, non-governmental organizations, and academia.[15] Stakeholders have acquired a body of knowledge and specific expertise that can inform needs-driven approaches based on their work with diverse communities. They work towards an effective and sustainable capacity building process, playing a key role in providing input on the cyberspace landscape, including the impact of cyberattacks, implementation challenges, and implementing the agreed norms in practice. These contributions are also essential for further developing and refining the Methodology.

The development of the Harms Methodology is a collaborative and multistakeholder process. The CyberPeace Institute has been consulting the research and design with a broad stakeholder community, including representatives from governments, industry, civil society, and academia. These consultations include seeking views on a range of issues, including how a methodological framework for measuring harm

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

could inform and improve the implementation of cyber norms. Such consultations in itself provide an important confidence building measure and increase the knowledge and capacity of participating States and organizations. Through this collaborative process and the resulting Methodology, we aim to better integrate the reflections on harms and impact into ongoing discussions about the implementation of the norms of responsible behaviour at the OEWG.

Finally, the CyberPeace Institute stands committed to supporting and informing the OEWG work based on its data-driven analysis, evidence-based recommendations, and the Methodology on impact and harms of cyber incidents. We actively seek opportunities to cooperate across the groups of stakeholders and extend our call for collaboration to governments and interested organizations and experts to gather their inputs on harm and impact stemming from the malicious use of cyber.

---

[1] The CyberPeace Institute is an independent and neutral non-governmental organization that strives to reduce the frequency, impact and scale of cyberattacks, to advocate for responsible behaviour and respect for laws and norms in cyberspace, and to assist vulnerable communities.

[2] CyberPeace Institute, "CyberPeace Analytical Report: NGOs serving Humanity at risk: Cyber Threats affecting 'International Geneva'," November 30, 2023, available at: https://cyberpeaceinstitute.org/wp-content/uploads/CyberPeace_Analytical%20Report_NGO.pdf; CyberPeace Institute, "Submission on the Protection of Humanitarian NGOs," March 1, 2023, available at: https://cyberpeaceinstitute.org/news/submission-oewg-protection-of-ngos/; CyberPeace Institute, "Submission on the Protection of the Humanitarian Sector," July 13, 2022, available at: https://cyberpeaceinstitute.org/news/submission-on-the-protection-of-the-humanitarian-sector-2/

[3] CyberPeace Institute, "Submission on increasing transparency around designations of Critical Infrastructure under Confidence Building Measures (CBMs)," March 7, 2023, available at: https://cyberpeaceinstitute.org/news/submission-oewg-designations-critical-

CyberPeace Institute
Campus Biotech Innovation Park
Avenue de Sécheron 15,
1202 Geneva, Switzerland

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

infrastructure-cbms/; CyberPeace Institute, "The role of confidence building measures (CBMs) in preventing escalation and strengthening cooperation for international peace in cyberspace," December 5, 2022, available at: https://cyberpeaceinstitute.org/news/the-role-of-confidence-building-measures-cbms/

[4] CyberPeace Institute, "Measuring harm from cyberattacks," December 11, 2023, available at: https://cyberpeaceinstitute.org/news/oewg-measuring-harm-from-cyberattacks/

[5] Cyber Incident Tracers provide independent, data-driven insights on the cyber threat landscape and the impact it has on people's lives. They are developed in-house with data sourced through the regular monitoring of open sources by our researchers. The information is made publicly available for use by policymakers and others and informs our work across the multistakeholder community. More information available at: https://cyberpeaceinstitute.org/cyber-incident-tracers

[6] CyberPeace Institute, "Report of Expert Meeting on the development of a Harms Methodology", December 20, 2023, available at: https://cyberpeaceinstitute.org/news/publications/report-expert-meeting-harms-methodology/

[7] Second Annual Progress Report of the OEWG, A/78/265, para 23.

[8] United Nations, General Assembly, UN GGE Report, July 22, 2015, available from: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement

[9] Second Annual Progress Report of the OEWG, A/78/265, para 42.

[10] Unpacking Cyber Capacity-Building Needs Part II. Introducing a Threat-Based Approach, UNIDIR, Authors Samuele Dominioni and Giacomo Persi Paoli, p. 15-16, available from: https://unidir.org/publication/unpacking-cyber-capacity-building-needs-part-ii-introducing-a-threat-based-approach/

[11] Ibid., p.39.

[12] Ibid., p.43-44.

[13] 2021 OEWG Final Report, A/75/816, para 56.

[14] Second Annual Progress Report of the OEWG, A/78/265, para 50.

[15] Second Annual Progress Report of the OEWG, A/78/265, para 51.