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

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

CyberPeace Institute's Statement

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

Measuring harm from cyberattacks

In anticipation of the sixth 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 on measuring harm from cyberattacks. This submission builds on the Institute's established work on the protection of NGOs[2] and critical infrastructure[3] and advances human-centric approaches to enforcing responsible behaviour in cyberspace.

We are pleased to outline our research and process on developing a standardised harm methodology – the progress made up to date in understanding the human costs of cyberattacks and the potential benefits of such a methodology for advancing accountability in cyberspace. **We further extend our call to States for collaboration to gather inputs on harm and impact stemming from the malicious use of cyber**.

Why is it important to measure harm?

The frequency, scope, sophistication and severity of cyberattacks have increased at an alarming pace in recent years, and will continue to do so, exposing vulnerable communities in particular. In relation to this exposure, there are many different terms

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

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

used – often interchangeably – to explain the resulting consequences, effects, impact, outcome, damage, and harm to the victims of such attacks.

Efforts to measure these consequences have predominantly focused on the direct impact on targeted systems or organisations; from time to restore, financial costs and to some extent the number of breached records. This narrow assessment of the impact of cyberattacks misses a fundamental element: **What harm do cyberattacks cause to people and society**.

The real harm to society and individuals is difficult to estimate, whether it has to do with a cumulation of many individual events or a one-off major disruption. There is currently no standard methodology in place, and we lack the metrics, tools, and frameworks to understand and track harm from cyberattacks over time. **This lack of evidence affects the ability to understand and measure the extent of the actual harm caused to people, and society.** It undermines a true evaluation of the scope and magnitude of such attacks and impedes policy making, resilience efforts – including resource allocation – and a means to affirm the real harm of a cyberattack for victims and in accountability processes.

Implementing the UN framework for responsible State behaviour in cyberspace

The 2021 Report of the UN Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (UN GGE)[4] calls for States to further advance transparency and predictability including through voluntary sharing by States of e.g. *"national approaches to classifying incidents in terms of the scale and seriousness of the incident"*[5], and *"…. frameworks … for identifying, classifying and managing ICT incidents affecting critical infrastructure"*[6].

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

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

The agreed-upon normative framework for responsible State behaviour in cyberspace also refers to relevant terms:

- *"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… …".*[7]

The UN Institute for Disarmament Research (UNIDIR) has provided a framework document[8] which 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"[9], and
- in relation to Norm F and G having a "Classification (public or non-public) of ICT incidents in terms of scale and seriousness"[10].

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

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

A standardised data-driven harm methodology and metrics to understand, track and measure the harm from cyberattacks could support these goals and practical implementation of the framework. **Such methodology can provide States with human-centric evidence towards building stronger and holistic accountability measures.**

Developing a standardised harm methodology

In 2022, the CyberPeace Institute initiated research and a process to develop a standardised harm methodology. **The strategic objective of this methodology is to identify means to measure and assess the harm of a single incident across multiple indicators and categories of harm.** This way, we can increase knowledge of the human costs, and influence policy, accountability and resilience efforts.

The CyberPeace Institute has undertaken research into categories of harm and indicators including those related to physical and psychological harm. This work leverages the Institute's repository[11] and analysis of cyberattacks against the healthcare sector since June 2020, and monitoring of cyberattacks in relation to an armed conflict. The Institute has further developed case studies that outline indicators of harm according to different categories determined by available data.

On 7 November 2023, the CyberPeace Institute convened a multi-stakeholder workshop on advancing the development of a standardised methodology to measure the societal harm from cyberattacks and monitor responsible behaviour in cyberspace. This event served as a platform for sharing the progress on a draft harm methodology, gathering expert input, and developing a shared understanding of the real harms and impacts of cyberattacks on people and society.

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

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

The upcoming report will provide observations and insights from experts and how this has confirmed and/or influenced the Institute's continuing work on this methodology.

The need for a collaborative approach

The harm methodology aims to strengthen capacities and design of evidence-based recommendations that can inform the OEWG work. It can support data-driven and human-centric approaches to monitoring responsible behaviour in cyberspace and become a practical tool for policy and decision makers striving to advance international peace and security in cyberspace.

To this goal, **the CyberPeace Institute seeks to continue to consult on its research, particularly on the harm and impact stemming from the malicious use of cyber**. This will allow us to further develop and refine the methodology.

Developing shared understandings of harm and impact in cyberspace will contribute to strengthening capacities and recommendations in multilateral negotiations mandated with the implementation of the normative framework. The insights drawn from the process of developing this methodology will also contribute to guiding broader cyber resilience and capacity building efforts.

Understanding the impact and harm that cyber incidents inflict on people will require a collective and coordinated response across diplomatic, policy, civil society and technical communities. The CyberPeace Institute remains committed to supporting and informing the work of the OEWG through multi-stakeholder and human-centric approaches and in close cooperation with governments and relevant stakeholders, to advance accountability, peace and security in cyberspace.

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

info@cyberpeaceinstitute.org
cyberpeaceinstitute.org

[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-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] Pursuant to paragraph 3 of General Assembly resolution 73/266.
[5] UN GGE Report, 2021, para 83.
[6] UN GGE Report, 2021, para 85.
[7] 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
[8] 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/
[9] Ibid., p.39.
[10] Ibid., p.43-44.
[11] 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.