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

Written Statement for the ICT Workstream First Consultation

Distinguished Delegates, Excellencies, and Colleagues,

Thank you for the opportunity to speak today on behalf of the CyberPeace Institute. I am honored to contribute to this important discussion on the use of Information and Communication Technologies in today's armed conflicts and, most critically, their human cost.

The CyberPeace Institute is an independent non-governmental organization based in Geneva, Switzerland, with a global mandate. Established in 2019, our mission is to reduce the harms from cyberattacks on people's lives by assisting vulnerable communities, analyzing cyber threats, and advocating for responsible behavior in cyberspace.

In my statement, I would like to contribute to this compelling discussion with reference to the core elements of our work that directly relate to the use of ICTs in armed conflict and their human cost. These are the Harms Methodology, which provides a structured way to assess the real-world impacts of cyberattacks on people, societies, and the critical infrastructure which they rely upon; our open-access Cyber Attacks in Times of Conflict Platform, which tracks cyber operations against civilian infrastructure in the context of the ongoing conflict, and our open-access CyberPeace Tracer, which tracks and analyze cyber threats and disinformation campaigns targeting civil society organizations (CSOs), including humanitarian organizations. Each of which is available to the public.

Through this work, we aim to bring a perspective that is grounded in concrete evidence and guided by humanitarian principles.

In recent years, the frequency, scope, sophistication, and severity of cyberattacks has increased at an alarming rate. Efforts to measure their impact, or "harm", have largely focused on direct effects to targeted systems or organizations, such as recovery time, financial losses, and, to some extent, the number of breached records. However, this narrow approach overlooks a

fundamental question: What is the true extent of the harm caused by cyberattacks to individuals, organizations, society, and international norms.

In other words, we identified a gap in our current understanding of ICT usage in times of conflict and the human cost that this was having. We also realised that this was having negative downstream effects, for a lack of comprehensive knowledge undermines the ability to assess the full scope and magnitude of cyberattacks. This obscures the real human and societal costs of cyberattacks, and in turn, hampers effective policy making, accountability, resilience-building to uphold international humanitarian law and better protect fundamental human rights.

To address this gap, the CyberPeace Institute has worked on the development of a standardized methodology to assess the harms and impacts of cyberattacks on people, society, and the environment.

The purpose of the Harms methodology framework is to be indicative of the harms in a given context rather than comprehensive. Instead of presenting prescriptive categories that presuppose certain kinds of harm, it is a descriptive tool for an analyst to organize the data that is available for the given incident. Starting at the high level, thematic groupings distinguish between the different kinds of entities that can be harmed, eg. individual, organizational, societal, international. The high-level groupings can then be divided into low level thematic groupings that are categorized by the type of harm, e.g. physical, psychological, economic, deprivation of rights and services, and reputational harm.

While the high-level groupings focus on who has been harmed, the low-level groups focus on the type of harm, and below the low-level groups are the indicators of harm. These indicators are the specific pieces of evidence or data demonstrating the type of harm caused by the attack. For example, a source suggesting that an individual had experienced “increased symptoms of Post Traumatic Stress Disease following a cyberattack” suggests that the threat actor had inflicted a psychological harm (low level harm) to individuals (high level harm).

A practical application of the harm methodology can be found on our Cyber Attacks in Times of Conflict Platform. Here, we systematically document cyber

incidents occurring in the context of armed conflict, with particular focus on those targeting civilian infrastructure essential to the survival of the population. Since early 2022, we have recorded thousands of cyberattacks and operations conducted by a broad range of threat actors, affecting individuals, organizations, and states across multiple regions. This documentation underpins our efforts to assess the human cost of cyber operations and highlight harm beyond the battlefield.

Furthermore, we are progressively introducing the harm and human cost assessment component into our CyberPeace Tracer – to analyze and expose how vulnerabilities, malware infections, phishing threats, AI-enabled digital threats, information operations and surveillance technologies such as spyware, are impacting organizations, their partners and beneficiaries. Hitherto, we have recorded eighty-four thousand threats impacting humanitarian organizations.

We have leveraged our data and expertise to contribute to high level policy processes, like the UN OEWG, we briefed the UN Security Council and the EU Parliament.

Drawing from our observations across multiple contexts of armed conflict, we have identified several key trends related to hybrid warfare:

- Firstly, there has been a steady increase in cyber operations that occur in parallel with kinetic military activity, often synchronized to maximize disruption.
- Secondly, control over digital infrastructure in contested areas has become a strategic objective, with efforts to manipulate information environments and restrict access to communication tools.
- Thirdly, cyber campaigns frequently extend beyond the immediate zones of conflict, impacting non-belligerent countries and sectors with no direct involvement in hostilities.
- Fourthly, the rise of ideologically motivated cyber actors and hacktivist mobilization has introduced a new dimension to modern conflicts, blurring the line between state and non-state activity.
- Fifthly, these operations often exploit civilian digital infrastructure, resulting in disproportionate impacts on vulnerable populations and critical services.

These trends in hybrid warfare showcase a modern conflict model where cyber and information warfare are central tools - highlighting the urgent need for international cooperation and robust cyber defenses. Importantly, much of this activity lies outside the scope of direct military engagement and often targets or incidentally affects civilian infrastructure, humanitarian organizations, and vulnerable populations.

We thoroughly support the ICRC in the effort to facilitate open dialogue and invite all actors – states, civil society, and international organizations – to continue collaborating in closing the knowledge gaps, upholding international law, and ensuring that the digital transformation of warfare does not come at the expense of human dignity and civilian protection.

Thank you.

Francesca Bosco
Chief Strategy and Partnerships Officer,
CyberPeace Institute.