Thematic Session: Existing and Potential Threats

The CyberPeace Institute has been documenting cyber incidents impacting humanitarian organizations, and civilian critical infrastructure, including the healthcare sector. States have recognised that the threat landscape is rapidly evolving with a rise in the frequency, sophistication, and intensity of cyberattacks.

The Annual Progress Report (APR) should highlight that cyber incidents against sectors of vital importance risk dire consequences in the form of harm and impact on people, and outline an ambition to increase the understanding of designations of critical infrastructure (CI). Furthermore, specific threats, especially ransomware and tools that can enable new modalities of cyber operations such as the use of large language models and generative AI that increases the capacity to carry out cyberattacks need to be examined in dedicated discussions that bring together a broad range of stakeholders in order to ensure appropriate controls and restrictions.

Ransomware has been underlined as a pre-eminent threat by a number of countries, as some ransomware incidents rise to a level that impacts international peace and security. Attackers can damage the operational capacity of critical sectors, affecting both States and private companies. Moreover, ransomware attacks, for example, on sectors that are custodians to sensitive data such as the healthcare sector and humanitarian action, have potential escalatory effects and can lead to multiple extortions against people in vulnerable situations. Double extortion has become the norm, involving both threats and data leaks in a complex cybercrime ecosystem, in which ransomware is often sold as a service. Preventing malicious activities requires
a whole-society approach, where the policies are informed by lived realities of victims, including from the industry, civil society, academia, and sector-specific experts.

The understanding of ransomware has largely been associated with economic or security impacts, with less focus on the societal impact. The CyberPeace Institute has been advancing human-centric research into the impacts and harm inflicted by cyber operations and attacks – stressing the impacts on people who are disproportionately targeted or affected in cyberspace and the differentiated harm stemming from cyberattacks that they may experience, e.g., based on their gender. We are also piloting a methodology that aims to measure harm from cyberattacks that could inform the work of the OEWG across the pillars of its mandate and advance accountability in cyberspace.

**Thematic Session: Rules, Norms and Principles of Responsible State Behaviour**

Voluntary norms are important for reducing unpredictability and potential escalation of conflict. However, an international instrument is only effective if it is implemented by States, through national and regional frameworks. States now need to “walk the talk” and take responsibility for implementing the commitments made.

Countries should develop concrete proposals to advance the implementation of cyber norms, especially those with high practical relevance – such as the commitment to not damage critical infrastructure (norm f) and the protection of their own critical infrastructure (norm g).

The APR needs to encourage States to present concrete proposals to advance norms implementation that can serve as a guidance to others, and we appreciate such an initiative currently being driven by the government of Canada.
Other supporting measures can help operationalisation of cyber norms, such as the “adopt a norm approach” building on the successful OSCE model of countries adopting confidence building measures (CBMs) and advancing them in practice. Furthermore, we encourage States to link each norm with targeted capacity building activities to help its implementation.

Stakeholders can provide context-driven guidance on the norm implementation. They advance the interpretation and clarification of existing norms and identify gaps in the operationalization of the framework of responsible behaviour in cyberspace. Moreover, Civil Society Organizations (CSOs) are well-positioned to build partnerships across a variety of actors and geographies to provide capacity building and help in the practical implementation of cyber norms.

CSOs conduct research based on proximity to victims, which helps build a body of knowledge about the impact and harm stemming from cyberattacks and operations. Together with other stakeholders, such as academia and private companies, they complement States’ analytical capacity regarding the potential effects of agreed-upon norms and their harmonisation with other existing frameworks.

The CyberPeace Institute has contributed to a number of joint initiatives with States and the private sector in support of operationalizing cyber norms. These partnerships reflect our shared commitment to advance the implementation of the framework of responsible state behavior through concrete multistakeholder action. The Institute aims to further monitor the implementation of the framework to foster accountability and transparency in cyberspace.

**Thematic Session: International Law**

Cyber operations and attacks are a reality in contemporary armed conflicts, including the targeting of critical civilian infrastructure. Mapping the cyber dimensions of the
ongoing armed conflict between the Russian Federation and Ukraine, the CyberPeace Institute has recorded 1,686 cyberattacks and operations by 95 different actors, impacting 23 critical infrastructure sectors and 48 countries globally. This translates to more than 23 cyberattacks per week.

This data collection and analysis raises serious concerns with regard to how States respect and abide by the existing legal framework, including domestic law, International Humanitarian Law (IHL), and Human Rights Law.

States must uphold their existing commitments under international law and the framework for responsible state behaviour in cyberspace. As agreed in previous GGE and OEWG reports the UN Charter and customary law are relevant to cyberspace. Countries have called for focused discussions on state responsibility under existing legal frameworks, to understand how these rules apply to the use of ICTs. The first APR states that “the OEWG could convene discussions on specific topics related to international law. This may include expert briefings, such as from the International Committee of the Red Cross, to consolidate common understandings on this subject.” However, these discussions have not taken place yet in the proposed format.

The CyberPeace Institute has conducted an analysis of how the legal and normative ecosystem relates to cyberattacks deployed during an international armed conflict. The complete analysis is publicly available on our Cyber Attacks in Times of Conflict Platform. It aims to support States in their work to develop and build upon their national views on how international law applies in the use of ICTs and also inform the work of the OEWG. By no means can the application of IHL be seen to permit weaponization of cyberspace. On the contrary, the application of IHL ensures protection for civilians and civilian infrastructure and aims to reduce suffering. There is an urgent need to discuss state responsibility under IHL, applicable to operations in the context of armed conflict, to understand how principles apply to the use of ICTs
by States. For example, in cases of impact on civilians, information operations, and civilian data.

Clarifications related to the interpretation of international law are still required by States. The proposal put forward by Canada and Switzerland to start discussions on how IHL, the UN Charter, and obligation of peaceful dispute resolution apply to the use of cyber is an important step forward. We further encourage States to form more informal, interregional working groups within the OEWG to advance concrete issues related to international law.

Stakeholders can be trusted partners in this regard. Several organizations have built a track record of elaborating how international law applies in cyberspace and thereby help to reach common understandings, for example, through independent expert briefings and roundtable discussions. Initiatives such as the Oxford Process on International Law Protections in Cyberspace provide important platforms for multi-stakeholder discussions on the clarification of how international law applies in cyberspace.

Civil society organizations and academia alike have important roles in research, capacity building and awareness raising. They are enabling and contributing to a rule of law ecosystem in which obligations are enforced with the cooperation of all parties, provide human rights expertise, and contribute to redress for victims of cyberattacks and we encourage States to reflect these multistakeholder contributions in the APR.

Thematic Session: Confidence-building Measures

At a time of rising concerns over the malicious use of ICTs by State and non-state actors globally, the effective operationalization of CBMs is key to an open, secure,
stable, and peaceful ICT environment. CBMs can contribute to incentivizing restraint and de-escalating tensions by providing transparency and building trust between and among States.

The CyberPeace Institute has called on States to advance CBMs in practice by providing more clarity on what constitutes critical infrastructure under their national frameworks. Increased transparency around critical infrastructure would contribute to greater predictability and enhanced trust and confidence between and among States. It could provide both incentives and tools for increasing the understanding of the threats to CI, advance national frameworks for strengthening and maintaining secure, functioning and resilient CI, and promote concrete and actionable discussions and practical cooperation in protecting CI through a multistakeholder approach at all levels.

States should also provide further information relevant to the framework of responsible state behaviour that would build common understandings, reduce tensions, and enhance the implementation of CBMs as an essential component of international peace and security. The non-exhaustive list of areas of potential additional transparency includes sharing information about cyber threats and vulnerabilities, national views on how international law applies in cyberspace, positive practices and existing capacity building initiatives, and national strategies and legislative frameworks related to the use of ICTs.

The Points of Contact (POC) directory that is currently under discussion at the OEWG can benefit from the experiences of regional organizations such as the Organization of American States (OAS) and the Organization for Security and Co-operation in Europe (OSCE). These organizations have acquired experience in creating and maintaining PoC directories in regional formats and leveraging capacity building through this network of contacts. Furthermore, the POC directory could also
gradually expand to include the contact information of relevant stakeholders to support more rapid crisis management, information sharing, and context awareness when cyber incidents take place.

Many non-state stakeholders are already driving initiatives with the aim of building trust and confidence between States and non-state actors. The ability of non-state organizations to actively engage in the OEWG process and exchange views with States in itself creates trust between Member States and the relevant organizations and experts, which is critical for the implementation of the framework. CSOs also provide research and monitoring of the application of CBMs in diverse contexts and encourage both public and private-sector stakeholders to provide clarity and transparency on their actions toward promoting a global culture of cybersecurity.

**Thematic Session: Capacity-building**

Cyber capacity building activities need to move beyond dispersed efforts and align with current assessments of threats and gaps in the implementation of the framework of responsible state behaviour in cyberspace. As an example, targeted capacity building can support sectors of critical infrastructure to increase protection and resilience. Focused capacity building and multistakeholder initiatives can be particularly beneficial for smaller countries with limited resources to help them assess which infrastructure is critical and how to protect it while leveraging the model of public-private partnerships.

Capacity building relevant to the mandate of the OEWG does not happen in a vacuum. Operationalising its principles necessitates identifying examples of good practices from what is already being carried out, as well as taking into consideration lessons learned from the operationalisation of principles in other fields. To tap into these synergies, projects building capacities of States need to be extended to non-state stakeholders. Many existing initiatives such as those building the knowledge around
the application of international law, are currently for state participation only. Stakeholders would benefit from broadening these initiatives and their inclusion would make such programmes more inclusive, transparent, informed, and impactful.

Stakeholders are already driving many capacity building initiatives. The Global Forum for Cyber Expertise (GFCE) creates a global multi-stakeholder community committed to sharing resources and practices. A number of CSOs, academia, and industry actors also focus their respective efforts to involve vulnerable and local communities for an effective building of capacities. Through their experiences, they can establish a level of trust between diverse actors and inform policy approaches with lived realities of cyber incidents.

The CyberPeace Institute has been assisting humanitarian and development non-governmental organizations (NGOs) through the CyberPeace Builders program. This initiative helps to prevent future attacks by identifying the vulnerabilities that attackers exploit and alerting NGOs about their risks and vulnerabilities, and helping them build cyber resilience. Furthermore, recognizing the growing and diverse needs of these sectors, the Institute launched the Humanitarian Cybersecurity Center to provide tools, expert support, and free cyber assistance to NGOs, tailored to their needs, through partnerships and networks of dedicated professionals and volunteers. Based on this successful model, we encourage States to support the culture of cybersecurity among NGOs and engage in broad multistakeholder participation to help build their resilience.

This year, the CyberPeace Institute is co-organizing the Global Conference on Cyber Capacity Building to elevate and mainstream cyber resilience and capacity building in the international development agenda. The event will take place in November in Ghana under the title “Cyber Resilience for Development”. This topic highlights the key role cyber resilience plays in supporting sustainable development, inclusive
economic growth, and social prosperity across regions. The call for proposals for sessions is currently open and we encourage all interested delegations and organizations to participate.

**Thematic Session: Regular Institutional Dialogue**

The Programme of Action to Advance Responsible State Behaviour in Cyberspace (Cyber PoA) reaffirms the commitment of States to implement the agreed-upon normative framework through an operative and action-oriented process. This format aims to promote peace, security, and stability in cyberspace through a cooperative model that advances the exchange of knowledge and practices, avoids duplication of efforts, and assists in national and regional implementation efforts.

The Cyber PoA will allow for the implementation of previous consensus reports of the Groups of Governmental Experts (GGEs) and OEWGs. It can support the implementation of all pillars of the framework of responsible State behaviour in cyberspace holistically and provide practical and needs-driven capacity building. Its mandate should include the implementation of cyber norms, building shared understandings of the applicability of international law, and operationalizing confidence building measures. Furthermore, it should offer flexibility to address additional issues that would benefit from information exchange, practical implementation and multistakeholder engagement.

Given the multistakeholder nature of cyberspace, civil society, industry, academia, and other experts must be part of a regular dialogue on cybersecurity. The Cyber PoA is an opportunity for a comprehensive engagement of the multistakeholder community, the inclusion of which can help to drive more impactful outcomes and
contribute to transparency, credibility and sustainability in the implementation of decisions.

The modalities for stakeholder engagement should be informed by other processes that have proven effective. Notably, the UN Ad Hoc Committee on Cybercrime has demonstrated an open and inclusive model that was agreed upon in the modalities of the participation of stakeholders in order to enable broad participation from civil society, the private sector, academia, and other relevant stakeholders.

While States bear the primary responsibility for the maintenance of international peace and security, non-governmental actors are their trusted partners that help effectively implement agreed measures and commitments. In anticipation of the regional consultations on the Cyber PoA’s scope, structure, and content, the CyberPeace Institute stands ready to inform the process in its expert capacity, and we look forward to exchanging with States and stakeholders in focused discussions on this issue.