Presentation to UN Member States on Existing and Potential Threats in Cyberspace_ CyberPeace Institute's Contribution

8 December 2020, Informal Multi-stakeholder Cyber Dialogue

Session on Existing and Emerging Threats

Key Points:

1. **What cyber/ICT related activities do you assess to be the biggest threats to international peace and security?**
    - Cyberattacks, operations, and threats that directly impact human lives and affect human security, dignity, and equity, should be the top priority of focus at the OEWG.
    - Security issues and threats addressed at the OEWG should move away from military and state centric approaches, and instead approach threats through a holistic, human centric perspective that considers the stability, empowerment, and development of people in cyberspace.
    - Reliance on ICTs in all aspects of society is only growing, and so there should be a concurrent growth in respect for, and commitment to due diligence by stakeholders to protect critical civilian infrastructure and avenues to promote accountability.
    - Stakeholders should ensure that the development and usage of technology will not hamper the participation of individuals and communities in their civil and political rights; as well as the assurance that individuals and communities will not be discriminated against due to bias, prejudice, and inequality.
    - In this regard, the worrying trend of attacks on the healthcare sector in the midst of the pandemic shows that there needs to be an increase in accountability in order to protect critical civilian infrastructure. This specifically relates to sectors that directly impact the security and dignity of humans, such as healthcare, food, and water, amongst others.

- Another worrying trend has been the development and increase in the sale and use of technologies to surveil and interfere with activists, advocates, and civil society organizations. Focus should be put on addressing these issues and holding relevant stakeholders accountable to their commitments. When ICTs are used to target those who work for the promotion of rights and issues for those most marginalized, it can have a serious impact on their work to develop dignity and equity for these vulnerable communities and therefore presents a worrying threat to peace in cyberspace.
- There is an urgency to shift the paradigm of technology development and threat assessments to a human-centric approach: when mass-scale produced technologies risk to fail to also meet the needs of the most vulnerable, this creates an exploitable vulnerability with possibilities for scaling attacks.
- In this regard, as every system is as strong as its weakest link, we cannot expect a safe cyberspace without ensuring that all actors from all communities have the necessary skills and knowledge to address cyber threats and to behave responsibly in cyberspace.
- Finally, as new technologies like artificial intelligence gain traction and usage across all sectors of society, from military deployments to state services and private sector products, there should be an emphasis on developing a sense of responsibility for all concerned stakeholders to ensure that the usage of such technologies does not impact the security, dignity, or equity of all peoples.

2. **With respect to the draft "Existing and Emerging Threats" section of the OEWG the pre-draft report, are there any notable omissions, additions, or statements with which you support or disagree?**
    - Threats to international peace and security leverage ICTs as a means for power projections, military activities, and malicious uses putting human security, dignity, and equity at risk. Current efforts to tackle cyber threats to international peace and security are failing to address the effective social

impacts and consequences of cyberattacks on vulnerable and affected communities. The CyberPeace Institutes praises previous efforts by Member States and other stakeholders in using a human-centric lens for policy-development and emphasizes the need to make this approach a standard analysis framework for discussions of security and peace in cyberspace. To this extent, in the following sections, the CyberPeace Institutes highlights important omissions to be considered for further discussions, as well as statements that support the Cyberpeace Institute's views and commitments:

- **Paragraph 17:** The misuse of ICTs and digital means with potential dual-use[1] features by terrorist and criminal groups represent an important threat to international security and peace. The CyberPeace Institute supports this statement and adds that the misuse of such technologies, especially those with censorship and surveillance means, can hamper human dignity and equity as well as democratic values and processes, and further adds that there should be emphasis that those who create these technologies have the obligation to ensure that their products are not used in manners inconsistent with responsible behavior and international law.
- **Paragraph 18:** The misuse of ICTs for purposes inconsistent with the UN Charter is strongly condemned by the CyberPeace Institute. The CyberPeace Institute supports this view and adds to this category of threats the spread of disinformation and misinformation in the form of infodemics which has shown a correlation with the increase of cyberattacks. Additionally, the CyberPeace Institute supports the concern for the pursuit of increasing automation and autonomy in ICT operations, and would like to iterate that advancements in technology should not be used in manners inconsistent with international law.

[1] Defined as "Dual-use items are goods, software and technology that can be used for both civilian and military applications". Definitions by the European Commission, available at: https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/index_en.htm

- **Paragraphs 19 and 20:** The CyberPeace Institute supports the view that awareness and adequate skills are required to effectively tackle cyber threats for international peace and security. In addition to this statement, the CyberPeace Institute would like to focus the attention of the international community on the need to ensure that developing areas which have recently experienced a wave of digitalization (and/or are going to be connected in the near future) have the necessary skills and knowledge to leverage the benefits of ICTs and digital means while being able to recognize risks and vulnerabilities.
- **Paragraph 22:** The CyberPeace Institute shares the view that attacks against critical infrastructures (CI) and critical information infrastructures (CII) have not only security implications but also economic and social ones. With this regard, the Cyberpeace Institute urges the international community to focus on the impact of cyberattacks on civilians and civilian targets[2] with a human-centric approach putting individuals and affected communities at the center of the discussions.

[2] Defined as the necessary infrastructure to access food, water, healthcare, sanitation,transportation services, and other sectors key to the civilians' lives and livelihoods.