SUBMISSION ON THE ROLE OF CONFIDENCE BUILDING MEASURES IN PREVENTING ESCALATION AND STRENGTHENING COOPERATION FOR INTERNATIONAL PEACE IN CYBERSPACE

to the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

Introduction

Cyber confidence building measures (CBMs) are designed with the aim to increase trust and understanding between states. The Annual Progress Report of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG II), adopted by consensus in July 2022, highlights the importance of recommending specific confidence-building measures proposing that “States make concrete, action-oriented proposals on CBMs”. The Annual Progress Report acknowledged that the OEWG serves as a confidence building measure.

At a time of rising concern over the malicious use of ICTs by State and non-state actors, and heightened geopolitical tensions, the effective operationalization and reinforcement of CBMs are vital and key contributions to an open, secure, stable, and peaceful ICT environment. Incremental steps can foster dialogue between States with the expectation to reduce the risk and impact of malicious activities in cyberspace. Such measures are essential for deepening common understandings, avoiding misunderstandings, reducing the risks of misperception and escalation, increasing predictability of state behavior and stability in cyberspace.
Building confidence is a gradual process, which requires the sustained engagement of UN member states, regional bodies, the private sector, the public sector, the technical community, academia, non-profits, and civil society organizations.

Regional organizations such as the Organization for Security and Cooperation in Europe (OSCE), the Organization of American States (OAS) and the ASEAN Regional Forum (ARF) in particular have developed and employed CBMs to reduce tensions stemming from the use of ICTs among their participating states. These intergovernmental organizations create invaluable platforms for sharing and exchanging information, facilitating communication, providing resources and exchanging best practices. These practical examples, including joint exercises, training, and lessons learnt should be acknowledged and built upon to further greater regional engagement including in other regions. Different actors can identify and consider the CBMs appropriate to their specific contexts and cooperate with states and non-state actors on their operationalisation.

**Increasing destabilization of cyberspace**

In recent years cyberattacks have been growing in scale, impact, and sophistication. The malicious use of ICTs by state and non-state actors is contributing to the destabilization of cyberspace and threatens the safe, secure, and trusted use of ICTs. Moreover, the risks of conflicts resulting from misperceptions between countries have become more acute as capabilities for cyber offense proliferate.

Notably, an increased number of cyberattacks and operations has been observed in relation to the international armed conflict between the Russian Federation and Ukraine. To date, the CyberPeace Institute has documented 730 cyberattacks and operations against 22 critical infrastructure sectors and affecting some 35 countries beyond the belligerent countries. The harm to people and risks of misperception, miscalculation or
misattribution in cyberspace have increased. This heightens the need and urgency for operationalization of CBMs to secure peace and stability in cyberspace.

The data collected by the CyberPeace Institute shows that cyberattacks and operations in relation to the armed conflict in Ukraine have impacted 22 different sectors essential for the survival of the civilian population – including health, public administration, energy, transport, financial and ICT. Such attacks disrupt critical services and impact civilians and other persons hors de combat. Attacks on critical infrastructure directly threaten the safety and well-being of people, thus all efforts must be made to ensure that state and non-state actors do not cause damage to critical infrastructure or impair its functionality.

**Information sharing and transparency measures**

CBMs can contribute to incentivizing restraint and de-escalating tensions between and among states, notably by providing transparency and building trust. Sharing, providing and exchanging information in open discussions is at the heart of building trust between various actors. Voluntarily provided information can include ICT threats and vulnerabilities, national views on how international law applies in cyberspace, national approaches to recognizing and defining critical infrastructure, including ICT-enabled critical infrastructure, best practices and existing initiatives, and national strategies and legislative frameworks in regard to ICTs, among others.

While determining what constitutes critical infrastructure is a national matter, transparency in this regard is important, and States should share positions on infrastructure considered critical. Putting forward designations of critical infrastructure can provide an opportunity for information sharing and mutual learning towards increased trust in cyberspace. CBMs could be key to strengthening the protection of critical infrastructure sectors.
The involvement of civil society can be particularly valuable in awareness-raising activities about CBMs, their role and implementation on various levels as well as in contributing to developing a shared taxonomy that can provide a clear definition of the cybersecurity context. For illustration, the CyberPeace Institute has compared the designations of critical infrastructure by a number of States. This highlights that definitions are very often general. Few States provide a list of sectors considered as critical, listing sectors such as nuclear, health, energy or food. As seen in the 2021 OEWG consensus report, and acknowledged by the 2021 GGE Report, the Covid-19 pandemic led a majority of States to take further action in protecting healthcare infrastructures. As more and more infrastructure become digitized, vulnerabilities to cyberattacks increase, and determining what constitutes critical infrastructure and refraining from targeting infrastructure is essential to protecting people.

**Strengthening cooperation**

Taking a broader perspective on the cyber threat landscape, the UN Member States should further advance the operationalization of the agreed CBMs and extend participation to relevant stakeholders. States should tap into significant technical and organizational expertise in the private sector and civil society to help ensure that CBMs are developed and implemented with multistakeholder input. Sharing current threat information that informs present and future confidence-building initiatives is one example of how to benefit from the specific knowledge and expertise that non-state actors bring.

Sharing lessons learned in different formats is also crucial to understanding the threat landscape, preventing cyber incidents, and avoiding escalations amid crises. Such exercises have an important awareness-raising component in regard to CBMs. Cooperation through consultations and engagement at all levels can contribute to advancing understanding and transparency between States, reduce distrust, and
Contribute to the peaceful mitigation of cyber incidents. Stakeholders such as the private sector, academia, civil society, and the technical community can contribute to or even facilitate such exchanges.

The goal of establishing Points of Contact (PoCs) is another concrete way to enhance the sharing of critical information, which is particularly relevant in cyber events with the risk of potential escalations. The inclusion of the private sector is promising and in line with promoting public-private partnerships and practical cooperation with relevant stakeholders.

PoCs can contribute to increasing cyber resilience and security of cyberspace, but it is important to consider that their effective functioning necessitates a capacity-building component that would harmonize the different levels of awareness, resources, and resulting capacity. Building capacity for CBMs should therefore be a priority in national development strategies, cooperation agreements regionally and through the UN.

Strengthening confidence and trust necessities progressing in other areas, including increasing clarity on implementing norms and applying international law. The framework of responsible state behavior in cyberspace must therefore be approached in its entirety to allow for an effective operationalization of CBMs as essential tools for enabling cyberpeace.

---


2 In strengthening the operability of PoCs it is important to share lessons learned between countries to assist those with less capacity and capabilities. This has been also highlighted in the UN General Assembly Resolution 73/27, “capacity-building is essential for cooperation of States and confidence-building in the field of ICT security” and “capacity-building measures should seek to promote the use of ICTs for peaceful purposes.”