UN SECURITY COUNCIL OPEN DEBATE ON CYBER SECURITY

Maintaining international peace and security in cyberspace

29 June 2021, 8:00 AM EDT
Location: VTC

I. Objective

The objective of this Open Debate is to contribute to a better understanding of the growing risks stemming from malicious activities in cyberspace and their impact on international peace and security as well as to address the global efforts to promote peace and stability in cyberspace. Member States will have an opportunity to reaffirm their commitment to international law and the framework of responsible State behaviour as key elements of conflict prevention and maintenance of peace and security in cyberspace.

II. Background

Pursuant to the UN Charter, the primary responsibility of the Security Council is the maintenance of international peace and security. Accordingly, the Council has paid attention to the evolving nature of challenges to international security by addressing a number of complex new factors that can destabilize countries and exacerbate or prolong existing conflicts. Over the years, the Council has held both broad thematic debates on new challenges to international peace and security as well as meetings dedicated to specific issues, such as climate change, natural resources, pandemics, famine, transnational organized crime and drug trafficking and piracy.

Although the Open Debate will be the first time the Security Council addresses cybersecurity as a separate issue, the Council has discussed the topic during several of its informal meetings and as part of a broader debate on international security. These meetings have demonstrated that for many countries cyber threats are a matter of concern and constitute a key security challenge. For example, in December 2017, under the presidency of Japan, the Security Council held an open debate on addressing complex contemporary challenges to international peace and security. During the open debate, the Secretary-General identified cybersecurity as one of the escalating dangers to international peace and security (S/PV.8144). In August 2019, Poland organised an open debate on challenges to peace and security in the Middle East and suggested that members consider "[h]ow to counteract cyber threats, including threats to energy infrastructure, in terms of promoting cooperative mechanisms for deterring and responding to significant cyber incidents in the Middle East" (S/2019/643), with several participants addressing this question in their interventions. Most recently, in April 2021, under the presidency of Viet Nam, briefers as well as several participants of the high-level debate on "Protection of civilians in armed conflict: indispensable civilian objects" (S/2021/415) pointed to the threats malicious cyber activities pose to critical infrastructure, notably medical facilities.

The free, open and interoperable cyberspace, managed and supported by the multi-stakeholder community, has undoubtedly allowed States to reap considerable economic value as well as promote social progress globally. Digital technologies have been an important catalyst for human progress and development. In addition, technology has served as an important platform

for promoting respect for human rights, giving a voice to vulnerable and marginalized groups of society. Sustainable digital development can also contribute significantly to promoting post-conflict stability in regional conflict zones.

Together with the growing dependence on the digital domain and the various benefits provided by digital transformation, there has unfortunately been a continuous rise in malicious cyber activities and growing systemic threats disrupting the functioning of critical infrastructure and digital services. The misuse of cyberspace can affect vital economic sectors and essential services to the public, such as healthcare and energy. This could lead to a potentially devastating humanitarian impact and risk having destabilizing effects that may threaten international peace and security. The COVID-19 pandemic has further increased reliance on critical digital infrastructure, underlining the importance of responsible State behaviour in cyberspace in accordance with the principles of international law.

In order to reduce the malicious use of cyber capabilities and build a more stable cyberspace, it is vital to follow relevant preventive mechanisms on a global, regional and national level. Over the last decade, UN Member States have made remarkable progress in formulating the elements of a normative framework for responsible State behaviour in cyberspace, premised on existing international law, norms, confidence-building measures and capacity building.

Existing international law, particularly the UN Charter, provides sufficient guidance for States on conducting cyber activities. Principles of international law that have successfully guided State behaviour in other domains offer also a primary reference framework for States in cyberspace. In addition to international law, voluntary, non-binding peacetime norms of responsible State behaviour and confidence-building measures also play a crucial role in providing guidance on State conduct in cyberspace, thus improving transparency, clarity and predictability. States must meet their obligations regarding internationally wrongful acts attributable to them under international law.

Experts under the UN First Committee have discussed advancing responsible State behaviour in cyberspace in the context of international security and have produced four consensus reports of the Groups of Governmental Experts (GGE) in 2010, 2013, 2015 and 2021.[1] At the UN General Assembly, Member States have agreed by consensus to be guided by norms for responsible State behaviour in their use of ICTs, as well as international law and CBMs.[2] The success of cyber processes in the UN First Committee in 2021 adds momentum for further implementing the framework for responsible State behaviour in cyberspace. The consensus report adopted in the UN Open-Ended Working Group (OEWG), endorsed by the UN General Assembly, reaffirmed the application of international law in cyberspace, norms, CBMs and capacity-building.[3] The consensus report agreed in the most recent GGE marked a significant contribution to deepening understanding on how international law applies, offering additional guidance on norm implementation as well as advancing confidence and capacity building in cyberspace.

Regional organizations such as the Organization of American States, the Organization for Security and Cooperation in Europe, the African Union, and the Association of Southeast Asian Nations, and the ASEAN Regional Forum have also made significant headway by adopting regional cybersecurity agreements as well as developing and implementing cyber confidence

[1] A/65/201, A/68/98*, A/70/174, endorsed by the UN General Assembly; the 2021 consensus report agreed on 28 May 2021 is yet to be given a document number
[2] UN General Assembly Resolution 70/237
[3] UN General Assembly Decision 75/564

building measures that aim to contribute to stability and to reduce the probability of escalation into conflict. Meanwhile, capacity building efforts and a wide array of global and regional programmes are playing a vital role in enhancing cyber resilience. Furthermore, given that States do not tend to manage their entire critical infrastructure themselves but rely on cooperation with the private sector, a number of public-private initiatives on cyber security have emerged. Taking into account the multi-stakeholder nature of cyberspace, any opportunities to involve the private sector, academia and civil society in global, regional and national discussions should be further encouraged.

III. Guiding questions

During the session, Member States may wish to address the following questions in their statements:

a) What are the present and emerging cyber threats to international peace and security? What kind of impact may the malicious use of cyberspace have in relation to conflicts in the future?
b) What global, regional and national policy mechanisms are in place to mitigate cyber threats and advance responsible State behaviour, and how can UN Member States effectively encourage their implementation?
c) How to strengthen compliance with existing international law and the implementation of norms of responsible State behaviour in cyberspace as agreed by UN Member States?
d) How to build confidence, reduce misunderstandings and prevent developments that could potentially lead towards a devastating humanitarian impact from malicious cyber activities?
e) During armed conflicts, how to mitigate possible humanitarian effects of the malicious use of ICTs?
f) Given the multi-stakeholder nature of cyberspace, what role can the wider community, including the private sector, civil society and academia, play in helping to prevent conflict, build common understandings and increase cyber resilience?
g) In the case of serious situations arising from cyber activities that might lead to international conflict or give rise to a dispute, what are the possible options to respond and seek a peaceful solution?

IV. Briefers

United Nations High Representative for Disarmament Affairs H.E. Ms. Izumi Nakamitsu has been invited to brief the Council.

V. Format

The High-Level Open Debate will be held on 29 June 2021 as an Open VTC. The Prime Minister of the Republic of Estonia, H.E. Ms. Kaja Kallas, will preside at the meeting.

All Member States of the United Nations that are not members of the Security Council and permanent observers to the United Nations are invited to participate by submitting written **statements through the e-Speakers module**. Member States should transmit their statements in Microsoft Word format with a cover letter duly signed by the Permanent Representative/Chargé d'affaires and addressed to the President of the Security Council no later than the date of the meeting, 29 June 2021. These statements will be published as part of an official compilation document containing the interventions submitted in connection with this open VTC.