United Nations S/2020/389

Security Council

Distr.: General
12 May 2020

Original: English

Letter dated 12 May 2020 from the Permanent Representative of Estonia to the United Nations addressed to the Secretary-General

I have the honour to inform you that Estonia is planning to hold an Arria-formula meeting of the Security Council on the theme “Cyberstability, conflict prevention and capacity-building” on 22 May 2020, from 10 a.m. until 1 p.m. The meeting will take place by videoconference. The concept note is attached (see annex).

I should be grateful if the present letter and its annex could be circulated as a document of the Security Council.

(*Signed*) Sven **Jürgenson**
Ambassador
Permanent Representative

Annex to the letter dated 12 May 2020 from the Permanent Representative of Estonia to the United Nations addressed to the Secretary-General

Concept note for the Arria-formula meeting on the theme "Cyberstability, conflict prevention and capacity-building", to be held on 22 May 2020

Organized by the Permanent Mission of Estonia to the United Nations, in cooperation with the Permanent Missions of Belgium, the Dominican Republic, Indonesia and Kenya to the United Nations

Objective

1. The objective of this Arria-formula meeting is to provide members of the Security Council with an opportunity to address global efforts to promote cyberstability and conflict prevention against the background of emerging cyberthreats. The meeting will be aimed at raising awareness of cyberchallenges in terms of international peace and security, and will allow for discussions on the global, regional and national policy mechanisms in place to mitigate cyberthreats and advance responsible State behaviour.

Background

2. Worldwide connectivity is growing rapidly. With 4.33 billion Internet users and 26 billion connected devices, the global digital ecosystem is enlarging at an unprecedented rate. The fast pace of digitalization has offered many opportunities for all our societies, and it is hard to overestimate the economic and social benefits of increased connectivity. The rapid expansion of the digital domain has also resulted in a critical dependency on the smooth functioning of digital services and infrastructure. In recent years, cyberattacks and incidents disrupting the functioning of critical infrastructure and digital services have grown in number and severity, contributing to a more uncertain international security environment. With cyberthreats on the rise, there is growing potential for instability and conflict. In the context of the ongoing global health crisis, the need to protect critical medical infrastructure and global Internet resources underscores the importance of bolstering security and stability in cyberspace.

3. In order to reduce the malicious use of cybercapabilities and to build a more stable cyberspace, it is vital to follow relevant preventive and normative mechanisms at the global, regional and national levels. Over the past decade, global discussions on responsible behaviour in cyberspace have taken place in many intergovernmental and multi-stakeholder forums. Norms of responsible State behaviour and the application of international law have been endorsed by the General Assembly. Regional organizations have been proceeding with the development of cyberconfidence-building measures that are aimed at contributing to stability and at reducing the probability of escalation into conflict. Several public-private initiatives on cybersecurity have sprung up, and the role of new technologies in international security is making its way into mainstream foreign policy debates.

4. United Nations Member States have already made remarkable progress in formulating the elements of a framework for conflict prevention and stability in cyberspace. The consecutive groups of governmental experts under the First Committee of the General Assembly have discussed advancing responsible State behaviour in cyberspace in the context of international security and have produced

three reports that were welcomed by the General Assembly, in 2010, 2013 and 2015.[1] In 2015, the General Assembly agreed by consensus in resolution 70/237 to be guided by norms for responsible State behaviour in the use of information and communications technologies. The ongoing discussions in the First Committee and in the two groups that were established under it – the Group of Governmental Experts and the Open-ended Working Group – facilitate the implementation of norms of responsible State behaviour and the application of international law and advance capacity- and confidence-building.

5. A number of 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, have achieved significant progress in adopting regional cybersecurity agreements and confidence-building measures. Regional organizations, such as the Organization of American States, have also spearheaded efforts to advance cyberresilience at the national level and to build technical and organizational capacity to deal with cyberthreats. Global consensus exists that capacity-building efforts should be increased to prevent potential attacks against critical infrastructure and to develop the policy and technical skills needed to secure the digital economy. Increasing national cyberresilience to address cyberthreats forms a primary building block of global cyberstability.

6. Another foundational element for cyberstability and conflict prevention is adherence to international law in cyberspace. Principles of international law that have successfully guided State behaviour in other domains are also a primary reference framework for State behaviour in cyberspace. International law can provide guidance on what conduct by States is acceptable in cyberspace, thus improving clarity and predictability for State behaviour. International law also contains a set of principles that could bolster cyberresilience for critical infrastructure.

7. Building on the Arria-formula meeting on the theme “Cybersecurity and international peace and security”, which was organized by the Permanent Missions of the Republic of Senegal and Spain to the United Nations in 2016, there is a need to further enhance this debate from the perspective of conflict prevention. With the United Nations cyberdiscussions continuing in many formats, the upcoming meeting on the theme “Cyberstability, conflict prevention and capacity-building” will be aimed at raising awareness regarding responsible State behaviour in cyberspace. The aim of the discussions will be to explore the existing norms, policies and cooperation mechanisms for advancing cyberstability, conflict prevention and capacity-building at the global, regional and national levels.

Briefers

- Under-Secretary-General and High Representative for Disarmament Affairs
- Senior Vice President and Director, Technology Policy Program, Center for Strategic and International Studies, James Lewis
- Chief Executive, Cyber Security Agency of Singapore, David Koh

Guiding questions

8. The following questions are proposed to assist Member States in preparing their statements:

[1] See www.un.org/disarmament/ict-security/.

(a) How have United Nations Member States implemented the cyberstability framework of voluntary norms of responsible State behaviour, confidence-building measures and international law thus far?

(b) What preventive measures could States take to enhance responsible State behaviour in cyberspace to create viable preconditions for the effective prevention of conflict stemming from cyberrisks?

(c) What kind of regional efforts support the observation of the norms of responsible State behaviour and the implementation of confidence-building measures, thus contributing to cyberstability and conflict prevention? What are the most prominent regional efforts to address cyberthreats?

(d) What global and regional mechanisms exist to contribute to better understanding and to provide an overview of capacity-building efforts? How could capacity-building be organized in a more effective way, considering the urgent need to build cyberresilience at the national level in many Member States? What are the requirements for cybercapacity-building in different regions?

Format

9. The meeting will be chaired by the Permanent Representative of Estonia to the United Nations, Sven Jürgenson. Following the opening statement by the Prime Minister of Estonia, Jüri Ratas, the briefers will deliver their presentations. The floor will then be given to the co-hosts and representatives of States members of the Security Council to make brief interventions. Time permitting, representatives of other United Nations Member States, permanent observers and non-governmental organizations may make interventions. Intention to take the floor should be indicated in the registration form, which should be sent to EEUNSC@mfa.ee by 18 May 2020. Interventions by representatives of Member States, permanent observers and non-governmental organizations should not exceed three minutes. Written contributions will also be welcomed and will be integrated into the summary of the meeting.

10. This Arria-formula meeting will be held by videoconference and will be live-streamed on YouTube, Facebook and on the website of the Permanent Mission of Estonia to the United Nations. The exact details will follow. The guidelines and technical requirements for joining the meeting will be shared with registered speakers in due course.