United Nations S/2020/643

Security Council

Distr.: General
6 July 2020

Original: English

Letter dated 2 July 2020 from the Permanent Representative of Estonia to the United Nations addressed to the President of the Security Council

I have the honour to transmit herewith the Chair's summary of the open Arria-formula meeting of the Security Council on the theme "Cyberstability, conflict prevention and capacity-building", which was held on 22 May 2020 (see annex).

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

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

20-08990 (E) 130720

Annex to the letter dated 2 July 2020 from the Permanent Representative of Estonia to the United Nations addressed to the President of the Security Council

Chair's summary of the open Arria-formula meeting of the Security Council on cyberstability, conflict prevention and capacity-building, held on 22 May 2020

Introduction

On 22 May 2020, Estonia, in cooperation with Belgium, the Dominican Republic, Indonesia and Kenya, organized an Arria-formula meeting on cyberstability, conflict prevention and capacity-building. In the light of the coronavirus disease (COVID-19) pandemic, the meeting took place by videoconference. The public meeting was live-streamed on several platforms to increase the transparency of the work of the Security Council. Fifty-two countries (one on behalf of a regional group) and three international organizations participated in the meeting. Two countries submitted written contributions.

The meeting was co-chaired by the Minister for Foreign Affairs of the Republic of Estonia, Urmas Reinsalu, from Tallinn, and by the Permanent Representative of Estonia to the United Nations, Sven Jürgenson, from New York. The opening statement was delivered by the Prime Minister of Estonia, Jüri Ratas. The Under-Secretary-General and High Representative for Disarmament Affairs, Izumi Nakamitsu, the Chief Executive of the Cybersecurity Agency of Singapore, David Koh, and the Director of the Technology Policy Program at the Center for Strategic and International Studies, James Lewis, briefed the participants.

The objective of the Arria-formula meeting was to provide members of the Security Council with an opportunity to address the global efforts to promote cyberstability and conflict prevention against the background of emerging cyberthreats. The meeting aimed to raise awareness of cyberchallenges to international peace and security and to discuss the existing global, regional and national policy mechanisms to mitigate cyberthreats and advance responsible State behaviour in cyberspace.

The present Chair's summary is not an official record of the meeting. It endeavours to provide a summary of the key issues, views and arguments expressed by the participants in the debate. It will be circulated to all members of the Security Council, as well as all delegations that participated in the debate. The statements of the participants can be accessed from a website of the Estonian Ministry of Foreign Affairs.[1]

Briefings

All briefers agreed that, while digital technologies brought great social and economic benefits, the growing digital dependency increased vulnerabilities and provided opportunities for conflict and crime. The COVID-19 crisis had made the need to bolster the security and stability of cyberspace even more topical and pressing. The crisis had shown that digital capabilities had become crucial for the provision of essential services, as well as for the continuation of effective governance. The disruption of the functioning of critical infrastructure could cause serious

[1] See https://vm.ee/en/activities-objectives/estonia-united-nations/signature-event-estonias-unsc-presidency-cyber.

consequences. The need to prevent such consequences and to ensure a stable and secure cyberspace had become a central issue for national and international security.

In the first briefing, the Under-Secretary-General and High Representative for Disarmament Affairs, Izumi Nakamitsu, noted that cyberthreats were an urgent issue and important progress had been made at the global level at the United Nations. Since 2004, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security had convened in five iterations and created a nascent global normative framework for the use of information and communications technology (ICT) by States. That framework included the following agreed elements: the applicability of international law, in particular the Charter of the United Nations, to the use of ICT; 11 voluntary non-binding norms of responsible State behaviour; practical confidence-building measures; and capacity-building measures. The discussions on the framework, its implementation and its further development were continuing in two First Committee working groups: the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts.

She pointed out that the active interest and engagement of States in the work of the working groups was an encouraging sign, as was the recognition of the urgency of the issue of ICT. Greater awareness, recognition and acceptance of the normative framework were also growing globally. The engagement of regional bodies, as well as of the private sector, non-governmental organizations and academia, was further positively contributing to the matter.

Despite the growth in awareness and recognition of the global framework, there was still room for improvement in its implementation. According to the High Representative, that could be done by cultivating partnerships, sharing experience, promoting common understandings on key issues and improving collective capacity-building efforts.

The second briefer, the Chief Executive of the Cybersecurity Agency of Singapore, David Koh, provided a national perspective towards achieving and maintaining a trusted and secure cyberspace. He said that Singapore was a small but digitally highly connected country with major banking, aviation and maritime industries. According to him, cybersecurity became more important when countries were more digitalized. Trust – towards Governments and international organizations, as well as among States – was one of the essential elements that ensured the functioning of a reliable digital space and had the effect of preventing conflicts. Critical information infrastructures that provided essential services to citizens as well as regular businesses needed to have the capabilities and measures in place to detect, respond to and recover from cyberthreats in a prompt and expedient manner. In order to preserve and increase trust in cyberspace, the international community needed to follow principles, norms and rules of responsible State behaviour and implement effective confidence-building measures.

He noted that in recent years there had been significant progress made in increasing possibilities for dialogue and collaboration at the United Nations level. Active engagement and substantive discussions, in the processes of both the Open-ended Working Group and the Group of Governmental Experts, on the norms of responsible State behaviour were building networks and mutual trust. In those dialogues, it was important to take a variety of views and voices into account; not just of States but also those of other stakeholders.

International and regional cybersecurity and cyberresilience required capacity-building within countries. According to him, regional organizations were ideally placed to undertake and lead such efforts. A good example was the Association of

Southeast Asian Nations (ASEAN) Cyber Capacity Programme (2016). ASEAN ministers and senior officials had also subscribed to the 11 voluntary and non-binding norms agreed upon by, among others, the Group of Governmental Experts in its 2015 report.

He concluded that a resilient and secure cyberspace could be achieved only through collaboration among Governments, the private sector, academia and civil society representatives. Cybersecurity should not be only about building defences but about developing infrastructure, capabilities and relationships.

The third briefer, the Director for Technology Policy at the Center for Strategic and International Studies, James A. Lewis, emphasized the importance of the framework for responsible State behaviour in cyberspace and the need to further accelerate the global adoption and observation of the voluntary non-binding norms in order to ensure a stable and secure cyberspace.

He provided an overview of the elements of the framework that had evolved since 1998, when the Russian Federation brought the topic to the United Nations, and in the discussions currently being held within the Group of Governmental Experts and the Open-ended Working Group. He suggested that the three reports of the Group of Governmental Experts – released in 2010, 2013 and 2015 – had provided a key contribution to the international discussion of security and stability in cyberspace and ultimately to a framework for responsible State behaviour. Those reports recommended that the Charter of the United Nations and international law guide State relations in cyberspace; they advocated cooperation between States and mutual assistance in case of significant cyberincidents. The reports encouraged the sharing of information on threats, vulnerabilities and vulnerability mitigations, and the building of cybercapacity. Crucially, the 2015 report of the Group of Governmental Experts, which was later affirmed by consensus by the General Assembly, proposed 11 voluntary norms as well as confidence-building measures to improve cybersecurity.

One of the central questions that he posed in his presentation was how Member States could both reinforce the ongoing processes (the Open-ended Working Group and the Group of Governmental Experts) and strengthen existing agreements on norms, confidence-building measures and capacity-building efforts to increase stability and security in cyberspace and thereby reduce the chances of conflict. He suggested that the best approach was to solidify and expand a shared understanding of what had already been agreed upon. For example, in his view, not enough attention had been paid to what would be appropriate consequences, consistent with international law and practice, for a decision by a State not to observe the 2015 norms. That was an area where agreement was likely to be determined by State practice rather than by a prescriptive or academic approach. In the examination and definition of State practice there was an important role for the Security Council.

Considering the growing importance of cybersecurity as part of international security, he proposed a set of points for future discussion by the international community. They included the development of a mechanism for regular institutional dialogue; strengthening the cooperation between regional and global as well as private initiatives; and defining appropriate responses to the non-observation of agreed norms.

Debate

Similarly to the briefers, the great majority of participants noted how almost every aspect of people’s lives had been affected by the rapid expansion of digital tools and services. Energy, transport and public utilities were all underpinned by digital technologies. The COVID-19 pandemic had only amplified the increasing reliance

and dependence on digital technologies in almost every sector of people's lives – medicine, education, communication and governance, to name just a few.

The increasing dependence on cyberspace, however, also brought about increased exposure to threats and vulnerabilities. Along with the rapid expansion of the digital domain, there had been a continuous rise in malicious cyberactivities and cyberincidents disrupting the functioning of critical infrastructures and digital services.

The participants emphasized that the need for a secure and safe cyberspace and the safety of critical services had become a concern. Cyberattacks against vital sectors and sensitive services risked having destabilizing effects and might ultimately threaten international peace and security.

A shared international understanding was needed of how to maintain a global, free, open, stable, peaceful and secure cyberspace, where human rights and fundamental freedoms and the rule of law applied. A large majority of States emphasized that a good foundation for stable and secure cyberspace had been established through the three consensus reports of 2010, 2013 and 2015 of the Group of Governmental Experts. Those reports outlined a framework of responsible State behaviour that was based on the application of international law, voluntary norms, rules and principles of responsible State behaviour, confidence-building measures and capacity-building. With those reports, the international community had recognized that existing international law applied to cyberspace.

Further discussions within the current Group of Governmental Experts and the Open-ended Working Group offered an opportunity to strengthen the common understanding of the application of international law and to support the further implementation and development of norms, rules and principles. That would facilitate State compliance, promote greater predictability and reduce the risk of escalation.

Many participants further elaborated that cyberstability was firmly rooted in existing international law; the Charter of the United Nations, international humanitarian law and international human rights law that applied to States' behaviour in cyberspace. Adherence to international law in cyberconduct included respect for and protection of human rights and fundamental freedoms online, just as offline. Some participants also emphasized that the applicability of international humanitarian law should not be undermined. International humanitarian law restricted States' conduct during an armed conflict and offered protection for civilians and civilian infrastructure. A small number of States expressed different views on the applicability of international law to cyberspace, reflecting the ongoing debates in the First Committee processes.

According to international law and the norms of responsible State behaviour, States should take appropriate action against actors that conducted malicious activities. Several countries also expressed a need to increase efforts to strengthen due diligence as well as accountability for State actions in cyberspace, in accordance with the 2015 norms of the Group of Governmental Experts.

Many participants stressed the necessity of strengthening global and regional cooperation to prevent conflicts and advance stability in cyberspace. The transboundary nature of cyberspace required cooperation that relied on relevant capacities within each State. At the global level, the United Nations played a crucial role in facilitating the discussion on cyberstability that could be maintained by ensuring an open, free, and secure cyberspace. At the regional level, organizations such as the Organization of American States, the Organization for Security and Cooperation in Europe, ASEAN, the African Union, the European Union, the Organization of Islamic Cooperation and the Cooperation Council for the Arab States

of the Gulf were mentioned as they had made great progress in implementing practical confidence-building measures in their respective regions, had improved cyberstability and had contributed to conflict prevention. Examples included the establishment of a point of contacts network, regular information exchanges, dialogue and sharing of best practices. The importance of cooperation between different stakeholders – the private sector, academia, civil society – was also emphasized.

A large majority of countries also found that, in order to increase cyberresilience, capacity-building was crucial. Capacity challenges ranged from the lack of awareness, varying understandings and interpretations, as well as technical capacity and financial constraints, to the implementation of existing voluntary and non-binding norms. Several States supported a coordinated approach to capacity-building that covered technical, policy and legal aspects along with adequate interaction and support from multi-stakeholder entities. Examples were provided of different capacity-building programmes that had often been conducted in coordination with international and regional partners and private sector stakeholders. Some countries highlighted the need to have a gender-sensitive and gender-diverse approach to capacity-building.

Several States outlined the measures and practices that they had adopted at the national level to combat cyberthreats and to put in place an adequate cybersecurity mechanism to strengthen domestic resilience in the cyber domain. Several States also mentioned the adoption of a national cybersecurity strategy and relevant action plans to increase the level of resilience to cyberthreats. Those strategies sought to improve the early detection of cyberrisks and emerging threats, thus making critical infrastructure more resilient to cyberattacks and reducing cyberrisks in general. Other measures included training programmes, national and international cybersecurity exercises and the adoption of national legislative frameworks.

Conclusions

The high number of participants, as well as their statements, supported the notion that cyberstability and cybersecurity are increasingly important to the foreign and security policy of States.

Malicious cyberactivities against vital sectors and services have destabilizing effects and may ultimately threaten international peace and security.

Since cyberthreats are largely transnational in nature, it is important to maintain international cooperation and dialogue between States, as well as between States and the multi-stakeholder community. It is through shared responsibility and joint efforts of Governments, private sector and civil society that we can effectively support the maintenance of international peace and security in cyberspace and protect human rights.

The United Nations plays an important role in driving international debates to raise awareness of cyberchallenges to international peace and security and to make progress on advancing responsible State behaviour in cyberspace.

A majority of States reaffirmed their responsibility to act in accordance with the international framework for responsible State behaviour in cyberspace as created by the three consensus reports of the Group of Governmental Experts, in 2010, 2013 and 2015, and as endorsed by the General Assembly. The three reports constitute an emerging cyberstability framework consisting of adherence to international law and the Charter of the United Nations, voluntary and non-binding norms of responsible State behaviour, confidence-building measures and capacity-building efforts.

Capacity-building and the strengthening of cyberresilience are other important elements in advancing global cyberstability. There is a need to address gaps in

cyberresilience among countries, both with regard to ICT infrastructure and the implementation of international law and cyberspace norms.

A majority of States also confirmed their interest in participating in further discussions at the United Nations on the stability and security of cyberspace, including through the Group of Governmental Experts and the Open-ended Working Group.

Despite the progress made, the growth in malicious cyberactivities and cyberincidents shows that there is a need for further discussions on how international law applies to cyberspace and how the norms of responsible State behaviour could be implemented. There is a need for States to increase their capacities in order to call out malign practices and impose accountability when rules are broken.