United Nations S/2024/446

Security Council

Distr.: General
10 June 2024

Original: English

Letter dated 7 June 2024 from the Permanent Representative of the Republic of Korea to the United Nations addressed to the President of the Security Council

I have the honour to transmit herewith the invitation letter and the concept note for the Security Council high-level open debate on "Maintenance of international peace and security: addressing evolving threats in cyberspace", to be held on Thursday, 20 June 2024, at 10 a.m. (see annex).

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

(*Signed*) Joonkook **Hwang**
Ambassador and Permanent Representative of the Republic of Korea
to the United Nations

Annex to the letter dated 7 June 2024 from the Permanent Representative of the Republic of Korea to the United Nations addressed to the President of the Security Council

I am pleased to invite you to the Security Council high-level open debate on "Maintenance of international peace and security: addressing evolving threats in cyberspace", to be held on Thursday, 20 June at 10 a.m., in the Security Council Chamber (see concept note). This will be the signature event of the Republic of Korea in its capacity as the President of the Security Council for the month of June.

Against the backdrop of rapid advancements in information and communications technologies, which have brought both benefits and challenges in our hyperconnected world, sophisticated and intrusive malicious cyberactivities are raising serious concerns for international peace and security. In this regard, the evolving security landscape in cyberspace demands the Council's keen attention in addressing cyberthreats that can affect all nations.

The high-level open debate will be chaired by the Foreign Minister of the Republic of Korea, Cho Tae-yul, and it will serve as a valuable opportunity for the Council to fulfil its primary responsibility of maintaining international peace and security in the era of expanding cyberthreats. High-level participation at this event will greatly enrich the discourse.

(*Signed*) Joonkook **Hwang**
Permanent Representative

Concept note for the Security Council high-level open debate on "Maintenance of international peace and security: addressing evolving threats in cyberspace", 20 June 2024, 10 a.m.

Background

While tremendous economic, social, cultural, civil and political benefits are brought by the advancement of information and communications technologies (ICTs), given our heavy reliance on digital infrastructure for communication, commerce and governance, malicious activities in the cyberdomain can undermine international peace and security, by affecting multiple domains simultaneously.

Malicious cyberactivities targeting critical infrastructure, including hospitals and other health-care systems, financial services, the energy sector, satellites, transportation and other emergency systems, are becoming increasingly commonplace. Such activities can have devastating effects on national security and pose substantial risk of harm to civilians. In addition to proliferation of malicious activities, evolving and advancing tactics including decoy ransomware, ransomware-as-a-service models and cryptocurrency thefts to support terrorist activities and to fund nuclear and other weapons of mass destruction programmes, are exacerbating the threat landscape, which is further compounded by the introduction of new vectors and vulnerabilities for exploitation.

While malicious cyberactivities are evident in a range of contexts, the use of these technologies in connection with, and in support of, armed conflicts is particularly worrisome. Malicious cyberactivities can both exacerbate existing conflict situations and support the initiation of new tensions.

With the transnational nature of cyberspace, no State is immune from the harms of malicious cyberactivities. The cybersecurity network is only as strong as its weakest link. In this vein, capacity-building is an indispensable element of cooperation across all relevant forums that address ICT-related issues within the United Nations system. A divergence in capacities or cyberresilience poses additional challenges for detecting, defending against, or responding to malicious cyberactivities, particularly for those States that have inadequate capacities. The harmful use of ICTs may have disproportionate effects on certain populations, including women and minorities.

Role of the Security Council

Progress

Over the past decade, the Security Council has become increasingly seized of the international peace and security implications of cyberspace. Since 2016, the Council has convened several Arria-formula meetings, during which States addressed cybersecurity with various linkages to topics such as protection of critical infrastructure, protection of civilians and disinformation and hate speech in cyberspace. Estonia convened the first high-level open debate on the topic in 2021, further solidifying the issue of the maintenance of international peace and security in cyberspace as a topic for the Council's consideration.

The most recent Arria-formula meeting on cybersecurity was organized by the Republic of Korea and co-hosted by the United States and Japan in April 2024. The meeting highlighted the growing implications of cyberthreats in the context of international peace and security, as well as the important role of the Security Council in de-escalating tensions and promoting cybersecurity.

Possible options

Developing a common understanding among States and enhancing the Security Council's role in addressing cyberthreats is both crucial and timely. Proactive engagement in cybersecurity, aligned with its primary responsibility to maintain international peace and security, positions the Council to respond to malicious cyberactivities and thus to significantly contribute to establishing a globally secure, open and peaceful cyberspace for the benefit of all nations.

Such an engagement by the Security Council can take place in a manner that is complementary to other ongoing United Nations processes on ICTs, including relevant discussions on norms of responsible State behaviour in the use of ICTs and the United Nations framework for responsible State behaviour in the use of information and communications technologies, which was adopted by consensus, under the auspices of the General Assembly.

Possible options for the Security Council's consideration were put forth at the Arria-formula meeting held in April, with a view to adding value to the various multilateral efforts that address the international peace and security implications of malicious cyberactivities.

For example, the Security Council could consider convening a briefing, ideally on a regular basis, to review the evolving cyberthreat landscape in relation to the existing mandate and agenda of the Council. Developing assessment and strategies on the evolving cyberthreat landscape by incorporating comprehensive insights from the United Nations system, the private sector, civil society and academia would ensure that the Council remains abreast of new developments and their implications for international peace and security.

Bearing in mind the inherent cross-cutting nature of international peace and security threats emanating from cyberspace, the Security Council could also explore ways to mainstream cyber- or ICT-related concerns when discussing country-specific files or other thematic files, such as peacekeeping and peacebuilding missions, Council-mandated sanctions, women and peace and security, or non-proliferation and counter-terrorism. Enhancing cyberresilience, strengthening national cybersecurity capabilities and promoting international cooperation could also be integrated into each of these lines of effort.

Furthermore, United Nations Member States could explore ways to enhance the Security Council's capacity to respond to the malicious uses of ICTs that pose threats to international peace and security, particularly those related to the protection of civilians, critical infrastructures and humanitarian efforts, ensuring a more holistic approach to the maintenance of peace and security.

Guiding questions

These questions may help guide Member State interventions:

- What are the key emerging and evolving trends of malicious activities in cyberspace that pose challenges to international peace and security?
- How does the malicious use of ICTs serve as a "threat multiplier" on existing conflicts and challenges in ways that necessitate the engagement of the Security Council?
- What specific roles and actions can the Security Council undertake to address international peace and security challenges emanating from cyberspace, and how can this role develop within its mandate in a mutually reinforcing and

complimentary manner alongside the existing work of other United Nations bodies? What are the required future steps?

- How are cyberthreats interlinked with other agenda items of the Security Council? How can the Security Council effectively mainstream cyber- or ICT-related concerns into its existing body of work?

Format and briefers

The high-level open debate will be chaired by the Foreign Minister of the Republic of Korea, Cho Tae-yul, and Council members are encouraged to participate at the ministerial level. In order to guarantee the participation of as many Member States as possible, statements should not exceed three minutes.

The following speakers will brief the Security Council:

- Secretary-General of the United Nations, António Guterres
- Stéphane Duguin, Chief Executive Officer, CyberPeace Institute
- Nnenna Ifeanyi-Ajufo, Professor of Law and Technology, Leeds Beckett University, United Kingdom

The list of speakers for the open debate will open at 9.30 a.m. on 14 June, the third working day preceding the date of the meeting. A letter addressed to the President of the Security Council, duly signed by the Permanent Representative or the Chargé d'affaires a.i., requesting to participate in accordance with rule 37 of the provisional rules of procedure of the Council must be uploaded to the eSpeakers module of e-deleGATE.