Permanent Mission of the Republic of Albania to the United Nations
New York

Concept note

United Nations Security Council Arria-formula meeting on: The responsibility and responsiveness of States to cyberattacks on critical infrastructure.

Organized by:	The Permanent Mission of Albania and the United States Mission to the United Nations.
Co-sponsored by:	The Permanent Missions of Ecuador and Estonia.

***

Date:	25 May 2023
Time:	3:00 p.m. – 5:30 p.m.
Location:	Trusteeship Chamber
Participation:	The Arria-formula meeting is open to all UN Member States, Observer Offices, Non-Governmental Organizations, and the press. Translation will be provided in all six languages. Co-sponsors, Member States, and Observer Offices will be invited to deliver statements after the briefers and Security Council Members. Priority will be given to co-sponsors and those speaking on behalf of groups of two or more delegations. To inscribe to deliver remarks, please provide the Member State name, speaker's name, and title to andris.stastoli@mfa.gov.al and garelleka@state.gov by 4 p.m. May 23. Participation at the Permanent Representative or Chargé d'Affaires-level is encouraged. Delegations are kindly requested to limit their interventions to 3 minutes.

***

Introduction:

The rapid development of digital technology has changed the way the world works, impacting all aspects of modern life. No doubt, this development holds benefits for everyone: from States and individuals to governments, industry, health and financial systems, regional and international organizations, and special political and peacekeeping missions.

Although the development of digital technology has many benefits, it comes at the cost of exposure to a wide range of threats. These threats arise from malicious cyber activities, by both State and non-State actors, and may endanger the maintenance of international peace and security. As a result, these threats could undermine the integrity, security, economic growth, and stability of the international community. Misuse of technology may escalate existing conflicts or cause new conflicts to arise. The cyber threat landscape is constantly evolving with the emergence of new technologies, such as artificial intelligence. Such cyber threats are increasing in a significant way and making the issue of cybersecurity more relevant than ever. This includes not only malicious cyber activities carried out for financial gains but also disruptive cyber incidents targeting States and their critical infrastructure.

International law, and in particular the Charter of the United Nations, applies to the activities of States in cyberspace. All Member States are obligated to uphold the Charter, including respect for human rights and fundamental freedoms, as well as other international law, including international humanitarian law, and should promote a global, open, stable, and secure cyberspace. All States have also committed to be guided by the Framework for responsible state behavior in cyberspace, including its eleven voluntary norms [A/RES/70/237]. Member States in the use of ICTs should also be guided by the reports of the Group of Governmental Experts, including its 2021 report, and the 2021 Report of the Open Ended Working Group on Development in the Field of Information and Telecommunications in the context of international security.

Of significant concern are malicious cyber activities aimed at critical infrastructure and critical information infrastructure facilities that affect essential public services within victim States. While the 2015 report of the Group of Governmental Experts on Advancing responsible State Behaviour in cyberspace in the context of international security (A/70/174) captured this concern as one of its eleven norms, cyberattacks on critical infrastructure continue to escalate in recent years.

Although States have conducted some of the most concerning cyberattacks impacting critical infrastructure, more of this activity can be attributed to non-state actors seeking financial gains. Even in the latter case, however, there is an expectation that States will not sit idly by. State

sovereignty and the principles that flow from sovereignty apply to the conduct by States regarding ICT-related activities and to States' jurisdiction over ICT infrastructure within their territory. Accordingly, there is an expectation that if a State is aware or is notified in good faith that an internationally wrongful act using ICTs is emanating from or transiting through infrastructure within its territory, it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation.

Cyberattacks that intentionally damage critical infrastructure or otherwise impair the use of such infrastructure to provide services to the public have an obvious impact on the maintenance of international peace and security. A State's failure to address potentially escalatory cyber activity emanating from its territory can also be destabilizing. In this context, and under the prevailing global circumstances, the Security Council must play a role in the assessment of the attendant risks and, above all, in the prevention of conflicts arising from the use of ICTs in cyberattacks. It must also promote responsible State behavior in cyberspace, and insist on adherence to the Charter of the United Nations and international law.

Objective:

In an interconnected world where States, public and private entities, and individuals rely ever more on services and operations offered in cyberspace, aspects of cybersecurity are intrinsically linked to international peace and security. This meeting aims to focus on the importance and relevance of addressing responsible state behavior in the use of ICTs as a matter of the Security Council's primary responsibility for the maintenance of international peace and security.

The Security Council must, with a view to discharging its duties under the Charter, take a leading role in promoting norms of responsible State behavior and underscoring the applicability of international law to Member State use of ICTs. By identifying and condemning counter-normative or unlawful State conduct and encouraging positive actions to improve the security and stability of cyberspace, the Security Council can reduce the risk of conflict arising from malicious actions or omissions. In particular, the Security Council should consider the uptick in cyberattacks on critical infrastructure and what further steps are necessary to deter this activity and mitigate the harm that it causes.

The meeting will be an opportunity to highlight contributions not only from States but also from other stakeholders, as well as speakers from international organizations who will provide information and enrich our action to overcome the current challenges related to cybersecurity. With so much of critical infrastructure owned and operated by the private sector, what is needed, at both the domestic and international levels, are real public–private partnerships in the service of combating cyber threats.

Briefers:

- **Ms. Izumi Nakamitsu**, Under-Secretary General and High Representative, UN Office for Disarmament Affairs
- **Ms. Marietje Schaake**, International Policy Director, Stanford Cyber Policy Center
- **Ms. Moliehi Makumane**, Cybersecurity Researcher in the Security and Technology Programme, UN Institute for Disarmament Research

Guiding questions:

- What are the possible actions the Security Council can undertake to address cyber threats and cyberattacks against critical infrastructure by States?

- What role can the Security Council play in ensuring a secure and peaceful cyberspace, in building trust between States in this regard, and in preventing conflicts arising from the use by any State or non-State actor of information and communication technologies for malicious purposes?

- What mechanisms do States have at their disposal to notify a second State of malicious activity emanating from its territory? What is the responsibility of the second State that receives such a notification?

- What mechanisms do victim States have to request assistance from other States in response to a severe cyberattack?

- What are the possible venues and mechanisms for a closer partnership between public and private entities for concerted and coherent defense and responses to cyberattacks?