



**UN Security Council Open Debate on Cyber Security:
Maintaining international peace and security in cyberspace**

**Remarks by Ms. Izumi Nakamitsu
High Representative for Disarmament Affairs**

Check against delivery



29 June 2021
VTC

Madame President,
Excellencies,
Distinguished delegates,

I wish to express my appreciation to Estonia for organizing this meeting and for inviting me to provide a briefing at this open debate on maintaining international peace and security in cyberspace.

As of January this year, there are over 4.6 billion active users of the internet worldwide. It is estimated that there will be 28.5 billion networked *devices* connected to the internet by 2022, a significant increase from the 18 billion in 2017.

As advances in digital technologies continue to revolutionize human life, we must remain vigilant in our understanding of malicious use of such technologies that could imperil the security of future generations.

Digital technologies are increasingly straining existing legal, humanitarian and ethical norms, non-proliferation, international stability, and peace and security.

They are also lowering barriers to access and opening new potential domains for conflict and the ability of both State and non-State actors to carry out attacks, including across international borders.

Specifically on ICTs, we have seen a dramatic increase in the frequency of malicious incidents in recent years. These incidents have come in many forms, from disinformation to the disruption of computer networks. Such acts are contributing to a diminishing trust and confidence among States.

These developments also pose a specific risk to critical infrastructure that are enabled by ICT technologies, such as the financial sector, electrical power grids and nuclear facilities. The Secretary-General has drawn attention to cyberattacks on healthcare facilities during the pandemic, calling on the international community to do more to prevent and end these new forms of aggression, which can cause further severe harm to civilians.¹

Such ICT threats also have a gendered impact and must be examined through this lens. Online violent extremism and trafficking have an often-overlooked differentiated impact on women, men and children, as do other ICT-related threats such as cyberstalking, intimate partner violence and the non-consensual dissemination of intimate information and images. This is also why we need to make every effort to secure the equal, full and effective participation of both women and men in decision-making in the digital arena.

ICT threats are increasing, but efforts are also underway to address them. Over the last one and a half decades at the United Nations, a series of five Groups of Governmental Experts, or GGEs, have studied the existing and emerging threats of ICTs to international security and recommended measures to address them. Two further UN processes, an Open-ended Working Group and a sixth GGE, both established in 2018, have recently and successfully concluded their respective work, taking important steps forward on the topic through the adoption of concrete, action-oriented recommendations.

These two Groups affirmed a suite of voluntary, non-binding norms of responsible State behaviour, recognizing that additional norms could be developed over time. They also reaffirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining

¹ <https://www.un.org/sg/en/content/sg/statement/2020-05-27/secretary-generals-remarks-the-security-council-open-debate-the-protection-of-civilians-armed-conflict-delivered>

peace, security and stability in the ICT environment. The Groups recommended confidence-building, capacity-building and cooperation measures, building on the work of previous processes. The Open-ended Working Group additionally, in accordance with its mandate, made conclusions and recommendations on establishing regular institutional dialogue on the issue of ICTs.

As the most recent GGE noted in its report, the measures recommended by the previous GGEs and the Open-ended Working Group together represent an initial framework for responsible State behaviour in the use of ICTs.²

A new, second Open-ended Working Group has also just held its organizational session and will begin its substantive work later this year.

At the regional level, regional organizations are now undertaking key efforts on ICT issues. Regional approaches have taken various forms as determined by different priorities and needs. Some regions have placed greater emphasis on implementing voluntary, non-binding norms of responsible State behaviour through capacity-building efforts, while others have pioneered their own regional confidence building measures to reduce the risks of conflict stemming from ICT activities or adopted other regional tools for addressing ICT threats. Various regional instruments are also in place addressing specific aspects of ICTs.

While States carry primary responsibility for maintaining international security, ICTs are an integral part of our societies and other stakeholders have a key role and interest, as well as responsibility, in securing cyberspace.

Many excellent private-sector-led cyber initiatives have been established such

² Para 21 of the GGE report. An advance copy is available at <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>

as the Cybersecurity Tech Accord led by Microsoft, the Charter of Trust led by Siemens and the Munich Security Conference, and Kaspersky Lab's Global Transparency Initiative.

The 2018 Paris Call for Trust and Security in Cyberspace brought together industry, States, civil society and academia in a commitment to nine Principles for cybersecurity. These Principles cover a range of issues from developing ways to prevent the proliferation of malicious ICT tools and practices, to the promotion of widespread acceptance and operationalization of international norms for responsible behaviour, as well as confidence-building measures for cyberspace.

Perspectives from the private sector, civil society and academia contribute a unique and important part of the collective solution to cybersecurity that the international community is seeking.

The United Nations, for its part, stands ready to support States together with other stakeholders in promoting a peaceful ICT environment. The Secretary-General convened a High-level Panel on Digital Cooperation which issued its report in 2019. Through a subsequent series of roundtable discussions with States and other key stakeholders, a Roadmap was developed, which recommended further actions to take forward cooperation in key areas in the digital space.

In the context of peace and security, the Secretary-General also launched an Agenda for Disarmament which places emphasis on understanding and addressing new generation technologies that pose possible challenges to existing legal, humanitarian and ethical norms; non-proliferation; and peace and security.

In his Agenda, the Secretary-General makes the commitment to engage and work with scientists, engineers and industry to encourage responsible innovation of science and technology and to ensure its application for peaceful purposes.

He also makes a second commitment to engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules and principles on responsible behaviour in cyberspace.

Distinguished Ministers and Delegates,

While the digital space has come to underpin almost every aspect of our daily lives, the scale and pervasiveness of ICT “insecurity” is also now recognized as a major concern. The political and technical difficulty of attributing and assigning responsibility for ICT attacks could result in significant consequences, including in unintended armed responses and escalation.

These dynamics can encourage States to adopt offensive postures for the hostile use of these technologies. It can also enable non-state armed and criminal groups and individuals seeking to develop or access potentially destabilizing capabilities with a high degree of impunity. Given these implications for the maintenance of international peace and security resulting from ICT threats, engagement by the Security Council on this issue is paramount.

I therefore welcome this opportunity to brief you, and I am looking forward to the discussion that will follow.

Thank you very much for your attention.