TO BE CHECKED AGAINST DELIVERY

Remarks of Dr Robin Geiss, Director, UNIDIR

At the Security Council Arria-Formula Meeting: "Evolving Cyberthreat Landscape and its Implications for the Maintenance of International Peace and Security"

4 April 2023, 3.00 PM (EST)

Distinguished Chair,
Members of the Security Council,
Excellencies,
Ladies and Gentlemen,

At the outset, allow me to express my gratitude to the Republic of Korea for convening this Arria-Formula meeting and for the invitation extended to the UN Institute for Disarmament Research (UNIDIR).

I also wish to thank the Permanent Missions of Japan and the United States for co-hosting this event, and to the UNODA Deputy Director Ebo for his insightful opening remarks.

This meeting is convened at a critical juncture for digital governance as the UN Summit of the Future is fast approaching and digital transformation accelerates globally.

Rapid technological advancements, including in artificial intelligence (AI) and quantum computing, hold immense promise of accelerating sustainable development for all. At the same time, our growing reliance on digital technologies makes us vulnerable to cyberattacks.

New technologies and dependencies offer malicious actors sophisticated means to disrupt critical societal functions, posing significant risks with potential implications for the Security Council's core mandate.

Last month, UNIDIR's annual Cyber Stability Conference, held at UN headquarters, gathered stakeholders from governments, the private sector, and civil society to discuss emerging cyber threats and their implications for international peace and security. Several key findings, underpinned by UNIDIR research, emerged from these discussions.

First, cyberattacks are becoming more sophisticated, more diverse, and more impactful.

Previously, cyberattacks focused on smaller and less protected targets and were relatively straightforward. Now, malicious actors employ complex tactics like polymorphic code, encryption, automation, and obfuscation to cover their tracks, deceive users, and bypass even advanced cybersecurity measures. They focus on a broader range of targets including government agencies, critical infrastructure operators, as well as ICT and industrial supply chains. As a result, a single successful cyberattack has the potential to disrupt service delivery for numerous users across multiple states, especially when critical infrastructure is targeted.

Cyberattacks on essential services – including water, energy, transportation, financial or healthcare – are well documented and can lead to severe societal disruption and significant human harm. For example, recent years have seen ransomware attacks on hospitals and threats to water systems, underscoring the domestic impact and international cascading effects of such malicious behavior.

Furthermore, cyberattacks targeting security and defense functions – whether conducted by state or non-state actors – can disrupt military command, control, and communication systems, affecting both conventional and nuclear armed forces in times of heightened geopolitical tensions. Such attacks, particularly if they are misattributed, can lead to miscalculation, escalation of tensions, and even trigger armed conflict.

We must also consider the gendered impact of cyber threats. Attacks on critical infrastructure and data disproportionately affect women and girls, who face a higher risk of being targeted online, through surveillance, doxing, online harassment, and hate speech.

The Secretary General's New Agenda for Peace recognizes this challenging threat landscape and calls on States to increase accountability in cyberspace and to ensure that services and infrastructure essential to the functioning of our societies remain off-limits. The Security Council has a crucial role in de-escalating tensions and promoting accountability when significant ICT incidents occur.

A second key trend is the emergence of cybercrime as a global service with a sophisticated division of labor and organizational structures.

Under this model, malicious actors can buy online cybercrime subscription services offering various attack methods – including ransomware, phishing, and denial-of-service techniques – as well as a range of supporting services such as a 24/7-available troubleshooting hotline. The cost of such a subscription on the dark web can be as low as $500 USD per year. This franchising of the global cybercrime economy, along with the rapid growth of a market for ICT vulnerabilities, has significantly lowered entry barriers for malicious actors.

In other words, cybercriminals now have ready-to and easy-to-use malicious tools and a range of supporting services to execute cyberattacks. This includes new variants of malware such as worms and file-less malware, which can spread without human intervention or use legitimate processes - such as software updates - to avoid detection and infect computers. The expanding use of spyware has also created an ever-growing market for cyber mercenary companies, hack-for-hire services, and ICT vulnerabilities, making these tools widely available to both state and non-state actors.

As a result, ransomware attacks increased approximately three-fold last year according to multiple cybersecurity vendors. The cost of such attacks to the global economy is also growing rapidly. Cybersecurity Ventures estimates that close to 8 trillion USD may have been lost to cybercrime disruptions in 2023 alone.

Most ransoms were paid in cryptocurrencies, which provide cybercriminals with anonymous and difficult-to-trace payment methods. Moreover, ransomware payments or assets gained through cryptocurrency mining and theft can provide actors access to internationally tradable currencies that can be used for financing terrorism, fueling armed conflicts, purchasing conventional arms, or developing weapons of mass destruction in contravention to existing UN Security Council resolutions and mandates.

During the previously mentioned Cyber Stability Conference, experts also highlighted that malicious actors are becoming more adept at using social engineering and manipulation tactics to maximize the effectiveness of cyberattacks.

This can include threatening public disclosure of personal data if ransom is not paid or exploiting public opinion trends to trick users into clicking on malicious links or opening infected email attachments. The exploitation of COVID-19 fears to drive phishing campaigns is a prominent example of the latter tactic.

As the third and final trend, technological advances, particularly in AI, are rapidly transforming the cybersecurity landscape. AI already helps cybersecurity professionals to stay ahead of emerging threats by analyzing vast amounts of signals from individual devices and proactively blocking new types of threats.

However, malicious actors are also utilizing AI to enhance the sophistication of cyberattacks, including by generating email phishing messages that can deceive even the most cybersecurity-conscious users and by using AI to guess and execute password attacks.

Moreover, the advent of quantum computing looms large on the horizon, with concerns that these advanced systems may both increase the resilience of digital systems and secure communications for some, but could also render modern cryptography obsolete and compromise cybersecurity for most.

In the future, unequal access to AI and quantum computing may have negative geopolitical implications, putting many countries at risk of falling behind in technology and cybersecurity, with potentially profound implications for international peace and security.

Excellencies,
Ladies and Gentlemen,

Cyberthreats are here to stay and will continue to evolve.

Given the interconnections between these threats and international security - recognized by General Assembly resolutions and Groups of Government Experts and the Open-ended Working Groups on ICT security - the Council Members could consider the following going forward.

First, the Council could follow its practice from other issue areas by convening a recurring annual session specifically dedicated to assessing the evolving cyber threat landscape and its implications for international peace and security.

To facilitate this process, as per the standard Council practice, the Secretary General could prepare a report outlining the latest trends and their estimated impacts on the Council's mandate to inform Member States' deliberations. UNIDIR, of course, stands ready to support any such efforts with its independent research capacity.

Second, as cybersecurity is a transversal issue, the Council could integrate cyberthreats into its existing workstreams and resolutions, including those on the protection of critical infrastructure, civilians in armed conflict, and humanitarian staff and objects.

Relatedly, the Council could task its expert committees to integrate considerations of how emerging ICT threats can undermine implementation of Council's resolutions into its reporting practices. The recent Security Council expert report on cryptocurrency theft and the funding of programs of Weapons of Mass Destruction serves as an important example in this regard.

Finally, the UN Security Council Members and the UN Membership more broadly could drive efforts to mainstream cybersecurity into broader discussions on digital transformation and sustainable development efforts worldwide.

Different States may face the same evolving cyber threat landscape, but the manifestation of risks will differ depending on the State's cyber resilience. Incidents across the globe illustrate significant technical, regulatory, and economic capacity differences and gaps that need to be addressed.

International cooperation and assistance, tailored capacity-building initiatives, and a joined-up approach of working together with all relevant stakeholders will be key to ensuring a cyber-resilient future for all.

UNIDIR stands ready to assist States in this crucial endeavor, whether through our research or the delivery of training and capacity-building programs on ICT security.

Thank you for your attention.