Permanent Mission of the Republic of Korea
to the United Nations

Permanent Mission of Japan
to the United Nations

ARRIA-FORMULA MEETING ON CYBER SECURITY

EVOLVING CYBER THREAT LANDSCAPE AND ITS IMPLICATIONS FOR THE MAINTENANCE OF INTERNATIONAL PEACE AND SECURITY

Organized by: Permanent Mission of the Republic of Korea

Co-hosted by: The Permanent Missions of the United States and Japan

Date and Time: 4 April 2024, 15:00-18:00

Location: ECOSOC Chamber

1. Background

Over the last several years, the Security Council has become increasingly engaged on the topic of cybersecurity. Estonia convened the first open debate during its Presidency in June 2021, and several Arria-Formula meetings were held featuring constructive discussions focused on, inter alia, malicious activities targeting critical infrastructure and the role of the normative framework for responsible State behavior in the use of information and communications technologies endorsed by the General Assembly.

While these meetings have proven highly beneficial for the Security Council and the broader UN membership, the threat landscape does not remain static, but rather continues to evolve and grow more complex; and thus merit ongoing consideration. In this vein, deepened exchanges on the landscape of existing and potential threats in cyberspace would greatly benefit the Security Council's consideration of their implications for international peace and security, simultaneously enriching its strategic response to these evolving security challenges.

2. Overview of the Evolving Threat Landscape

From a proliferation of malware, use of decoy ransomware to deploy wipers to disrupt diverse sectors including critical infrastructure, to the theft of cryptocurrency and other sensitive information, the threat landscape continues to be redefined not only by the nature of the threats themselves, but also by the expansion in the number and spectrum of threat actors.

Ransomware

Ransomware attacks were traditionally considered financially motivated and the consequences were erroneously underestimated both in terms of quantity and quality. Ransomware continues to proliferate,[1] and data from 2023 shows a major escalation in the frequency, scope, and volume of ransomware attacks. Ransomware is costly for both the

[1] The Second Annual Progress Report of the Open Ended Working Group contained in A/78/265

public and private sectors, and its consequences are not limited to stealing money, virtual assets, intellectual property, and important data.

High-profile ransomware attacks against government institutions and key critical infrastructure such as hospitals and healthcare systems; and energy, satellite, and other emergency services, were proved to have far-reaching impacts on public safety and political stability. The ransomware attack against Korean Hydro and Nuclear Power in 2014, the WannaCry incident in 2017, and the ransomware-as-a-service attack on Colonial Pipeline in 2021 showcased the severe impact of ransomware on essential public services and the vulnerability of complex, interconnected ecosystems.

Hackers deployed massive ransomware attacks on various government institutions in Costa Rica, to the extent that the government had to declare a State of emergency. The attackers further threatened to overthrow the government; clearly manifesting their political motive. Recent cases of hacking and breaches targeting government institutions and international organizations further aim to leverage or even exacerbate existing geopolitical tensions and conflicts, and can potentially have detrimental effects on democracy, governance, and human rights.

Cryptocurrency

Malicious cyber actors continue to target and attack financial institutions, ranging from national banks to cryptocurrency-related firms, to generate illicit revenues. Hackers not only distribute ransomware and malware to breach into financial systems, but also utilize criminal and fraudulent techniques such as phishing campaigns, romance scams, and social engineering to target people in relevant industries and steal money and data from them.

Cryptocurrency heists provide a transformative edge for malicious actors and serve as a major source of illicit revenue. 2023 was a record-high year in terms of cryptocurrency payments to ransomware actors, exceeding 1 billion USD, and scams associated with cryptocurrency generated an estimate of $4.6 billion USD in revenue in 2023 alone.

Such activities require heightened attention from the Security Council and the international community, in that these illicit gains from ransomware and cryptocurrency heists are used to fund the development of nuclear weapons programs or even finance terrorist activities. For instance, one Member State's illicit gains from malicious cyber activity account for approximately half of its foreign currency revenue, and about 40 percent of its Weapons of Mass Destruction (WMD) programs are known to be funded by illicit cyber means. Nation-States and non-State actors sanctioned by the UN Security Council are increasingly leveraging gains from cybercrimes as a vital tool to evade UN Security Council-mandated sanctions regimes, undermining the effectiveness of the collective work of the Security Council.

Expansion of Malicious Actors

Modern cyber threats have become even more complex in terms of the expansion of actors both vertically and horizontally. This trend was enabled by easier access to tools and techniques such as supply chain attacks, where a malicious code is inserted into trusted software updates, and Ransomware-as-a-Service (RaaS) models, which enable even non-state actors such as “cyber mercenaries[2]” to launch ransomware campaigns. Experts believe that Artificial Intelligence will also lower the barrier of entry for malicious cyber actors, who can take advantage of the technology.

A Call for International Cooperation

In light of the current threat landscape, there is a “grey area,” or a “cross-over,” where criminal behaviors in cyberspace have growing implications on international peace and security. This necessitates a more comprehensive and holistic assessment by the international community, and it is an issue the Security Council can rightly consider; given its primary responsibility of maintaining international peace and security.

No State is immune to malicious activities carried out in cyberspace since such threats are inherently borderless. The most vulnerable are often those with less developed technological and institutional capacities to prevent, mitigate, and respond to such incidents. Thus, open, inclusive discussions on the threat landscape are in the interest of all States; necessitating further discussion on international cooperation and capacity-building efforts.

3. Objectives:

- To raise awareness of the Security Council members and other Member States by examining the latest evidence-based research and horizon scanning on cyber threats, such as ransomware, crypto-heists, and financial crime involving advanced cyber-techniques, as well as their potential impact on both public and private sectors globally.

- To promote better understanding of the impact of various malicious cyber activities, that were characterized as cybercrime, on international peace and security, including WMD non-proliferation, which includes actions characterized as cybercrime and other existing disarmament architecture, and Security Council-mandated sanctions.

- To discuss and provide possible recommendations on enhancing the UN Security Council’s pivotal role and comprehensive engagement in addressing the multifaceted nature of cyber threats, in a manner that compliments and creates synergy with the ongoing work and discussions of relevant UN General Assembly Committees and Specialized Agencies, including the ones on Framework of Responsible State Behaviour in Cyberspace.

4. Guiding Questions:

- What are the key emerging and evolving trends of malicious activities in cyberspace that pose additional challenges to international peace and security, including, but not limited to, the use of ransomware, crypto-heists, and the stealing of sensitive information and other assets through cybertechniques like phishing?

[2] companies and sometimes individuals dedicated to developing, selling, and supporting offensive cyber capabilities, including surveillance technologies that enable their clients to spy on networks, computers, and other devices.

- How can criminal activities in cyberspace serve as a threat multiplier, exacerbating existing threats and challenges to international peace and security?
- How does the increasing accessibility of advanced cyber tools and techniques, previously limited to State actors but now available to a broader range of both State and non-State actors, impact international peace and security?
- What collective measures, including existing and innovative tools, platforms, frameworks, or strategies can the international community leverage to counter threats such as ransomware and cryptocurrency heists that endanger international peace and security? What is the necessary capacity-building efforts in this regard?
- What specific roles and actions can the UN Security Council undertake to address the evolving nature of cyber threats effectively, within its mandate of maintaining international peace and security?

5. Briefers:

- **Director Adedeji Ebo,** UN Office of Disarmament Affairs(UNODA)
- **Dr.Robin Geiss,** Director of the United Nations Institute for Disarmament Research(UNIDIR)
- **Ms. Valeria Kennedy,** Director of Intelligence Solutions for Investigations and Special Programs at Chainalysis Inc

6. Format

- **Participation**: Open to all UN Member States, Observer Offices, Non-Governmental Organizations, and the Press

- **Translation:** Will be provided in all six languages, but only until 18:00 (strict)

- **Webcast:** Via UN Web TV

- **For Statements:** Member States and Observer Offices will be invited to deliver statements after the briefers and Security Council Members. Delegations are **kindly requested to limit their statements to 3 minutes**. Priority will be given to speakers on behalf of groups of two or more delegations.

  Please note that due to time constraints, we may not be able to make it through the entire speakers list. A summary of the meeting with the statements enclosed will be prepared and officially circulated as a Security Council document.

  To be inscribed on the speaker's list, please provide information related to Member State(s), speaker, and title to unrokdisarmament@gmail.com and hglee13@mofa.go.kr **by 2 April 18:00**. Participation at the Permanent Representative or Deputy Permanent Representative level is encouraged.