Nations Unies S/2024/445

Conseil de sécurité

Distr. générale
12 juin 2024
Français
Original : anglais

Lettre datée du 6 juin 2024, adressée au Président du Conseil de sécurité par le Représentant permanent de la République de Corée auprès de l'Organisation des Nations Unies

À la suite de la réunion sur la cybersécurité organisée selon la formule Arria par la République de Corée, sur le thème « Évolution des cybermenaces et incidences sur le maintien de la paix et de la sécurité internationales », qui s'est déroulée le 4 avril 2024, j'ai l'honneur de vous faire tenir ci-joint un recueil de toutes les présentations et déclarations des États Membres qui ont participé à la réunion, dans la langue d'origine utilisée par les orateurs et oratrices (voir annexe).

Le recueil a été organisé suivant l'ordre de prise de parole des orateurs et oratrices ; on y trouvera aussi les déclarations prononcées sous forme abrégée ou qui n'ont pas été prononcées eu égard aux contraintes de temps.

Je vous serais reconnaissant de bien vouloir faire distribuer le texte de la présente lettre et de son annexe comme document du Conseil de sécurité.

L'Ambassadeur,
Représentant permanent
(*Signé*) Joonkook **Hwang**

* Distribuée uniquement dans les langues de l'original.

24-10177 (F) 200624 260624

Annexe à la lettre datée du 6 juin 2024 adressée au Président du Conseil de sécurité par le Représentant permanent de la République de Corée auprès de l'Organisation des Nations Unies

Security Council Arria-formula meeting on cybersecurity

Evolving cyberthreat landscape and its implications for the maintenance of international peace and security

Presentations and statements
4 April 2024

List of speakers

I. Briefers

United Nations Office for Disarmament Affairs (UNODA) – Director and Deputy to the High Representative, Mr. Adedeji Ebo

Distinguished Chair,
Members of the Security Council,
Excellencies,
Dear participants,

Let me begin by thanking the Republic of Korea for the invitation to brief on such a timely topic: the evolving cyber threat landscape and its implications for the maintenance of international peace and security.

I also wish to express thanks to the co-hosts of the event—the Permanent Missions of Japan and the United States.

Mr. Chair,
Threats emanating from cyberspace are of direct relevance to us all— individuals and governments alike—as our lives grow more “digital” by the day.

The Internet of Things grows unabated with more than 7 billion connected devices and an expectation that this number will balloon to 22 billion by 2025.

Government institutions increasingly rely on digital technologies for the provision of public services.

Supply chains and critical infrastructure are being digitized.

Rapid developments in cloud computing capabilities, quantum technologies and artificial intelligence are revolutionizing how businesses function.

At the global level, digital technologies present tremendous opportunity for sustainable development—from combatting climate change to eradicating poverty.

With each technological advance, there is an opportunity to improve how we communicate, educate and more.

But expanding dependence on digital technologies also brings distinct vulnerabilities and risks.

From a proliferation of malicious software such as malware, wipers and trojans, to a diversification of techniques such as spearphishing and distributed denial- of-service attacks, the cyberspace threat landscape continues to grow more complex.

When such risks pose a threat to international peace and security, whether as a result of impacts on critical infrastructure, humanitarian organizations or political or electoral processes, the implications are serious and can be escalatory.

In particular, malicious cyber activity targeting critical infrastructure and critical information infrastructure can have cascading effects at the subregional, regional and global levels.

Beyond its effects on the population, such activity can undermine trust and confidence in public institutions and impact the general availability or integrity of the Internet and data, leading to further tension, escalation and even conflict.

In the current environment, ransomware is becoming an increasingly potent threat.

Ransomware incidents with the potential to pose a threat to international peace and security are on the rise, including those targeting critical infrastructure and government institutions with far-reaching effects on the public and private sector.

Such activity can have reverberating impacts across the supply chain, and on the sectors that need to be protected the most, such as healthcare.

While techniques transform, so does the configuration of threat actors.

The ease of access to digital technologies makes the potential pool of actors practically boundless.

While there is broad recognition that a number of States are developing cyber capabilities for military purposes, including for intelligence, disruption and destruction,

there is also rising malicious activity involving non-State actors, including terrorists and criminal organizations.

Non-state actors, including criminals, terrorists, hacker groups and individuals, continue to utilize diverse tools, techniques, exploits and attack vectors to cause disruption and destruction to networks, applications and content.

There is also the growing challenge of “cyber mercenaries”—companies and sometimes individuals dedicated to developing, selling and supporting commercially available cyber intrusion capabilities, including surveillance technologies.

The market for such intrusive capabilities is widening.

Exacerbating the threat landscape is the convergence of rapidly advancing technologies, which is creating new vectors for exploitation and revealing novel vulnerabilities.

Integration and convergence of such technologies, from artificial intelligence and autonomy to quantum technologies, can both create new threats and significantly strengthen existing ones by increasing their frequency, scale or effect.

There are also potential benefits of such technologies for enhancing cybersecurity, such as for threat mitigation.

For example, post-quantum cryptography has been identified as a key method to ensure the continued security of transmitted and stored data, while AI can detect vulnerabilities at a transformative pace.

All this is to say, the cyber threat landscape is complicated and becoming increasingly so.

The international community, however, is not without tools to address these challenges.

The General Assembly remains fully seized of the challenges posed by State use of information and communication technologies in its dedicated open-ended working group.

Through this group, States continue to address questions of responsible State behaviour in cyberspace and the applicability of international law to State activity in this domain.

With the adoption of two consensus annual progress reports, the Open-ended working group is demonstrating its tremendous value.

From establishment of an intergovernmental points of contact directory to elaboration of concrete confidence-building measures, actionable outputs have emerged.

States also continue to unpack existing and emerging threats to the ICT environment.

States have acknowledged that not only is the use of information and communications technologies in future conflicts becoming more likely, but such technologies have already been used in this context.

States are also actively considering the cumulative and evolving framework for responsible State behaviour in the use of information and communication technologies, which provides a solid basis for responding to both existing and emerging threats.

While the General Assembly continues to play an indispensable role in these efforts, the Security Council can complement this work.

From the first high-level debate on cybersecurity in 2021 to the latest Arria- Formula on activity impacting critical infrastructure in 2023, the Council is becoming increasingly engaged in these matters.

Such discussions enrich our understanding of the threats and lay the groundwork for more effective responses.

The Security Council can also undertake practical actions like raising awareness of the agreed normative framework of responsible State behaviour and address questions of accountability for malicious activity.

This year will provide several opportunities for States to address questions related to cyberspace.

In the lead-up to the September 2024 Summit of the Future, a multi-stakeholder process to elaborate a Global Digital Compact is underway.

'A Pact for the Future' is also under negotiation, including discussions on tackling challenges emanating from emerging domains like cyberspace.

We would do well to maximize efforts across all these fora—from the General Assembly to the Security Council—to safeguard the safety and security of cyberspace.

Distinguished Chair,
Members of the Security Council, Excellencies,
Dear participants,

A growing diversity of threats, compounded by the agile adaptivity and sophistication of techniques, make our work of unpacking the threat landscape challenging.

Of course, a fundamental challenge to understanding the threat landscape is its dynamism.

Fully understanding the threats is somewhat of a moving target—as the threats evolve, so must our understanding.

Thus, this "Arria-Formula" meeting is an important opportunity for in-depth discussions with contributions from experts.

In this regard, I very much look forward to the contributions of colleagues from UNIDIR and Chainalysis Inc.

I thank you for your attention.

United Nations Institute for Disarmament Research (UNIDIR) – Director, Dr. Robin Geiss

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.

Chainalysis – Ms. Valeria Kennedy

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

I wish to begin by thanking the Republic of Korea for convening this timely Arria Formula meeting as well as Japan and the United States for co-hosting this event. I am honored to be here today to represent Chainalysis, the blockchain intelligence platform, in this important dialogue.

As denoted by my insightful co-briefers, offensive cyber activity is not just a tool for opportunistic cyber criminals and hacktivists, it is also being deployed by highly capable state and state-sponsored threat actors. Malicious cyber operatives have the potential to cause economic damage, wreak havoc on critical infrastructure, conduct espionage, facilitate sanctions evasion, fund weapons programs and terrorism, and undermine trust in global systems essential for modern society. As such, addressing the multifaceted challenges of cybersecurity has become paramount in safeguarding international peace and security in the digital age.

Cryptocurrency is built on blockchain technology and propels a cyber campaign through each stage of the killchain. Tools and services like infrastructure and domains are bought and sold with cryptocurrency generated through illicit cybercrime such as ransomware and cryptocurrency theft. After a successful campaign, threat actors reinvest their profits into additional purchases of access, brute forcing tools, botnets, and the like. Thus, one key way to measure the activity of cyber forces is through blockchain analytics because blockchain technology is inherently transparent.

Chainalysis data shows that 2023 saw a 94% jump in ransomware payouts from the previous year, hitting an all-time high. These are record-setting incident numbers and underscore a major escalation in the frequency, scope, and volume of ransomware attacks. In 2023, ransomware actors targeted high-profile institutions and critical infrastructure, including hospitals, schools, and government agencies. These attacks were not only financially motivated, but often politically motivated. Major ransomware supply chain attacks were carried out last year, such as the ubiquitous file transfer software MOVEit, which impacted companies ranging from the BBC to British Airways.

As a result of these attacks and others, ransomware gangs reached an unprecedented milestone, surpassing $1 billion in extorted cryptocurrency payments from victims.

The chart on the screen plots each ransomware variants' median ransom size versus the frequency of successful attacks. We see that the winning strategy in 2023 was big game hunting, where sophisticated actors focused on fewer and larger institutions with deeper pockets, with the aim of a higher payout. We also see strains like Phobos adopt the Ransomware as a Service (RaaS) model. Ransomware as a Service is a ransomware business model where operators develop and sell tools to affiliates, who launch attacks and in exchange pay the strain's core operators a cut of the ransom proceeds.

Initial access brokers penetrate the networks of potential victims, then sell that access to ransomware attackers for as little as a few hundred dollars. Initial access brokers combined with off-the-shelf ransomware as a service operators lower the barrier to entry for less technically sophisticated hackers, and can be a force multiplier, enabling ransomware groups to carry out a large quantity of these smaller attacks and rack up profit.

Examples are on the graph on the left on the screen. This shows a ransomware operator paying several initial access brokers. This actor later perpetrated attacks worth millions of dollars. Ransomware attackers often try to rebrand to distance themselves from strains publicly linked to sanctions or that have incurred too much scrutiny. Rebrands and affiliate switching can also allow attackers to hit the same victims twice under different strain names. On the right, we see an example of this: three actors that were not known to be affiliated are actually connected on-chain.

While North Korean hackers also conduct ransomware attacks, they excel at cyber espionage and theft. They target a multitude of organizations to obtain technical information to advance its Weapons of Mass Destruction and missile program and cryptocurrency businesses to steal virtual currency assets.

North Korea-linked hacks have been on the rise over the past few years, with cyber-espionage groups such as Kimsuky and Lazarus Group utilizing various malicious tactics to acquire large amounts of crypto assets. In 2023, we estimate that DPRK stole slightly over $1.0 billion worth of cryptocurrency, but the number of hacks rose to 20 — the highest number on record. $1.0 billion represents the value of digital assets at the time of the exploits. There is still a significant amount of stolen funds actively being

laundered, as the value of cryptocurrency has sharply increased in the last couple of months so too has the value of DPRK cryptocurrency holdings.

The majority of attacks in 2022 were on DeFi protocols, which are decentralized financial systems built on the blockchain. However, this took a turn in 2023, when DPRK diversified their attacks with cryptocurrency exchanges, centralized services and wallets. This could be attributed to an improvement in DeFi protocols' security practices.

North Korean hackers deploy patterns of techniques, including gaining initial access via social engineering and phishing. One example of social engineering is shown on screen: this is a Kimsuky actor spoofing a think tank employee and utilizing a spoofed domain in order to target another employee. Once the target responds with input, the Kimsuky actor sends a follow-on email with a malicious attachment.

These groups also rapidly evolve in how they actually move funds from a platform. With increased security measures adopted by crypto platforms, state actors need to find more advanced ways to break in. These cyber actors spend a long time in their targets' networks, observing business operations, and looking for opportunities to steal significant funds. Their ability to rapidly evolve, as doors are closed to them, continues to make them an advanced persistent threat (APT).

In June 2023, thousands of users of Atomic Wallet, a non-custodial cryptocurrency wallet service, were targeted by a hacker, leading to estimated losses of $129 million. The FBI later attributed this attack to North Korea-affiliated hacking group TraderTraitor and stated that the Atomic Wallet exploit was the first in a series of similar attacks, including the Alphapo and Coinspaid exploits later in the month. Following the Atomic Hack, the North Korean affiliated hacking group went through a complex laundering process in an attempt to evade detection. On the screen, you see some of the techniques that were utilized, which are common in these types of attacks.

For example, after stealing cryptocurrency from thousands of wallets, the group swapped from one cryptocurrency to another at centralized exchanges and bridges, which are cryptocurrency services that allow users to trade their assets and swap to other blockchains, such as Tron or Bitcoin.

The attacker sent their ill-gotten funds to an OFAC sanctioned mixing service called Sinbad that has been previously used by North Korean money launderers. A crypto

mixer is a service that blends the cryptocurrencies of many users together to obfuscate the origins and owners of the funds.Funds were ultimately sent to high-activity addresses on Tron, a cryptocurrency on a decentralized blockchain. These addresses likely belong to over-the-counter traders. Over-the-counter cryptocurrency trading facilitates direct trades between two parties without the use of an intermediary; these parties can convert cryptocurrency into other cryptocurrency, or provide a cash-out opportunity from cryptocurrency to fiat currency.

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 as reported by the UN Panel of Experts. Nation-States and non-State actors sanctioned by the UN Security Council are increasingly leveraging gains from illicit cyber activities as a vital tool to evade UN Security Council-mandated sanctions regimes, undermining the effectiveness of the collective work of the Security Council.

The cyber threat landscape is borderless and ever-evolving. Combating sophisticated threat actors requires swift and coordinated global action. To safeguard against hacks, robust security practices and rapid response mechanisms must be implemented, particularly in the face of persistent threats like phishing and social engineering tactics employed by state actors. Within the realm of cryptocurrency, proactive measures such as on-chain activity monitoring, cybersecurity tools, stringent compliance measures, and training allow crypto platforms to react quickly to exploits and facilitate law enforcement interventions and disrupt illicit fund flows. As the industry matures, aligning with fiat counterparts in terms of sanctions compliance becomes imperative, necessitating strong control frameworks and regulatory enforcement. Disrupting the ransomware supply chain through targeted interventions and focusing on the individuals driving these attacks are essential strategies for mitigating their impact. Moreover, global collaboration and information sharing are vital for building a resilient cybersecurity ecosystem and countering cyber threats effectively on a global scale. Chainalysis stands by to support these efforts.

Thank you for your attention.

II. Co-hosts

The Republic of Korea

Thank you, Madame Co-Chair.

I would like to thank Director Ebo, Dr. Geiss, and Ms. Kennedy for their insightful briefings.

The development of information and communication technology (ICT) has brought immense benefit to our hyper-connected, digital way of living. However, “the brighter the light becomes, the darker the shadow gets.” The more we are digitally connected, the more we become vulnerable to illicit cyber activities.

Several features of cyberspace present unique challenges for the international community. Cyberspace defies the conventional concept of physical space, making geographical distance irrelevant. The speed of digital interaction enables simultaneous actions all across the globe. The low cost of operation and lower entry barriers for various actors, coupled with the ambiguity in attribution, create conditions prone to abuse of deniability and difficulty in a collective international response to threats in cyberspace.

Taking advantage of these inherent characteristics of cyberspace, malicious actors and their criminal techniques in cyberspace are constantly evolving.

The advent of artificial intelligence, Ransomware-as-a-Service (RAAS) or other types of so-called “cyber mercenaries,” can avail sophisticated cyber capabilities for individuals, terrorist groups, and transnational criminal syndicates.

Accordingly, the cyber threat landscape is also rapidly changing, and its implications for international peace and security continue to grow. Against this backdrop, allow me to highlight the following three aspects of malicious cyber activities pertinent to the mandate of the UN Security Council.

First, ransomware attacks, which are traditionally underestimated as merely financially motivated and criminal in nature, are now an emerging threat in the context of

international peace and security. Large-scale ransomware attacks on critical infrastructure can have serious national security implications by leaving hospitals, energy plants, financial services, communications, transportation, and other essential service sectors and entire governments damaged and dysfunctional. My own country, the Republic of Korea, also suffered large-scale ransomware attacks in the past years. Costa Rica declared a state of emergency in 2022 after suffering a massive ransomware attack. And two years ago, a ransomware attack on one Member State even led to the severance of diplomatic ties with the Member State accused of that attack.

Ransomware can potentially exacerbate existing conflicts and geopolitical tensions. In addition, commercial spyware is increasingly misused to target government officials or human rights activists for illicit surveillance purposes, jeopardizing core values such as freedom, human rights, democratic principles, and the rule of law.

Second, States or non-state actors under UN sanctions are increasingly relying on illicit cyber activities to evade Council-mandated sanctions, eroding the effectiveness of the Security Council's tools at its disposal. The recent annual report by the Security Council's 1718 Committee Panel of Experts, whose mandate comes to an end this month due to Russia's irresponsible veto, discovered that the DPRK's malicious cyber activities generate about 50% of its foreign currency income; effectively evading the stringent financial sanctions imposed by the Security Council. Malicious non-state actors are also using cryptocurrency and the Dark Web to finance terrorism and to make unlawful weapons purchases. All in all, Security Council-mandated sanctions, including asset freezes and arms embargoes, are becoming untenable in the face of illicit cyber activities and misuse of virtual currency.

Third, illicit cyber activities can pose additional challenges to the global non-proliferation architecture. A textbook example in this regard is the DPRK's malicious cyber activities. About 40% of the DPRK's WMD programs are funded by its illicit cyber activities according to the aforementioned Panel report. Over 50 Member States have now been directly affected by a DPRK-backed hacker groups that have breached into networks of foreign banks and crypto agencies.

The DPRK's elite hackers have been illicitly acquiring intellectual property from major defense companies, including from those of their closest allies, to develop WMD programs and their delivery systems. The Panel of Experts report clearly describes the

indiscriminate nature of the DPRK's Defense industrial base targeting. From European aerospace companies to Russian Satellite Communications Company, the hackers have tried to obtain sensitive information including designs and blueprints of WMDs and missiles.

Distinguished Delegates,

With the widened spectrum of both malicious actors and their activities, it is fair to say that there is a "grey area" where there is a cross over between the traditional concept of cybercrime and cybersecurity.

The Security Council can address the topic of cyber threats, focusing on its mandate and primary responsibility conferred by the UN Charter, in a complementary manner with the preexisting mandates and work of the respective Committees of the General Assembly on cybersecurity and cybercrime respectively. The Security Council must take a leading role in raising awareness of the ever-changing threat landscape and its impact on international peace and security, and further deter and address such threats through a comprehensive approach. The Security Council's pivotal role in catalyzing deliberations on emerging threats is already proven in the case of resolution 1540 on the challenge of non-state actors' possible acquirement of WMDs.

Given the transnational nature of cyberspace, the chain of cyberspace is only as strong as its weakest link. Thus, international cooperation and capacity-building with developing countries are essential in our collective efforts to respond to cybersecurity threats.

Distinguished Delegates,

New technologies always bring us both benefits and challenges. Utilizing emerging technologies without proper understanding of their potential threat implications is costly. Bearing this in mind, the Security Council should fulfill its responsibility by actively engaging in the agenda of cybersecurity, laying the ground for more effective responses. We sincerely hope that today's meeting can serve to build momentum moving forward. As one of the world's most digitally connected countries, The ROK will spare no effort in bringing fresh insights on this matter of ever-growing significance. Thank you for your attention.

Japan

I thank Ambassador Hwang for his leadership, and Japan is pleased to co-host this meeting.

Also, I thank the distinguished briefers for their informative contributions.

We have seen a rise in cyberattacks targeting the foundations of our societies, including disruption or destruction of critical infrastructure, interference in foreign elections, ransom demands and steal of sensitive information, even in the form of state-sponsored cyberattacks.

Cryptocurrency theft poses a significant threat, with $1.7 billion stolen globally last year, according to industry reports, potentially funding illicit activities like WMD and missile programs.

Ransomware's transnational reach threatens national security, finance, and personal data protection.

Additionally, the proliferation of commercial cyber intrusion tools, like spyware, raises questions and concerns over its impact on national security, human rights and fundamental freedoms, international peace and security, and a free, fair, and secure cyberspace, broadening access to dangerous capabilities that can be misused by malicious actors.

Malicious cyber activities may also pose a significant threat to nuclear power plants or even nuclear command and control systems, which could lead to an unimaginable nuclear catastrophe.

International cooperation is not an option but an absolute necessity for all of us.

Japan attaches great importance to the current Open-ended Working Group (OEWG) as an inclusive platform under UN auspices.

That being said, allow me to outline Japan’s priorities on ICT governance.

First, **a greater role for the Security Council**.

The Council must closely monitor any situations involving serious cyber incidents that have grave consequences for international peace and security, including those targeted at critical infrastructure.

Also, the Council must pay closer attention to the growing cyber threats to the global arms control and non-proliferation regime.

With greater access to advanced cyber technologies, States could misuse such tools to illicitly finance their weapons programs, or they could simply steal the blueprints for weapons.

One notorious example is North Korea's WMD and missile program.

The 1718 Committee Panel of Experts has provided fact-based, independent assessments and analysis, and its recent report once again confirmed that North Korea has been conducting malicious cyber activities such as cryptocurrency theft and illicit financial operations to fund their WMD program.

In this context, we regret that the mandate renewal of the Panel was vetoed by a permanent member of the Council.

However, we must continue to work together to ensure the full implementation of all relevant Security Council resolutions on North Korea.

Cybercrimes and malicious cyber operations can also be used by terrorists or any other non-State actors.

The work of the 1540 Committee must also be continuously updated to effectively address emerging WMD proliferation challenges posed by non-State actors.

Second, **the rule of law in cyberspace**.

We stress the importance of upholding existing international law in cyberspace through concrete discussions about how international law applies in the cyber domain, rather than pursuing new legal instruments.

Another primary task of States must be to consider how to implement and operationalize our agreed norms, rules, and principles of responsible State behavior.

Third, **confidence-building measures**.

Enhancing mutual understanding among States can help mitigate the risk of tensions or escalation. In this regard, Japan welcomes the recent establishment of the global Points of Contact.

Fourth, **capacity-building**. Japan is fully committed to the promotion of capacity-building and will provide constructive and practical contributions to the Global Roundtable on capacity-building scheduled for May.

In conclusion, let me reiterate that Japan is firmly committed to safeguarding a free, fair, and secure cyberspace. The Security Council must remain seized more frequently on the emerging security risks associated with ICTs.

I thank you.

The United States of America

Thank you, Ambassador. I will now speak in my national capacity.

Once again, I am grateful that we've gathered to discuss this critical matter of peace and security.

Let's start with the good news: Already, States have made commitments to address malicious cyber activity.

The UN's Framework for Responsible State Behavior – adopted repeatedly and by consensus – makes clear that international law applies in cyberspace, and offers guidance and norms on how states can act responsibly.

That includes an expectation that States investigate and mitigate malicious cyber activity emanating from their territory, and aimed at the critical infrastructure of another. So that when ransomware actors in one State continually target, say, hospitals in another, that activity does not go unaddressed.

Colleagues, this is not a hypothetical. We have seen a significant spike in ransomware attacks on hospitals and health care organizations here in the United States, causing disruptions to everything from prescription refills to vital surgeries.

And yet, despite the expectation that States investigate ransomware actors on their soil, some members – most notably, Russia – have looked the other way, or worse, empowered those malicious actors.

In addition to Russian activity, the United States is also concerned about the DPRK's malicious cyberattacks. The UN 1718 Committee Panel investigations found 17 cryptocurrency heists in 2023 for which the DPRK may be responsible with losses valued at more than $750 million.

Those heists follow 58 similar suspected DPRK cyberattacks in the six years prior, with cryptocurrency companies counting some $3 billion in losses.

And let's be clear: It's not just that this money was stolen. Revenues from the DPRK's cyber operations, including work to steal or launder foreign currency directly funds its unlawful WMD and ballistic missile programs. To say nothing of the DPRK cyber operations aimed at intimidating North Korean escapees.

Now, it's not just the DPRK or state actors. Previously, this technology was prohibitively expensive to acquire, and prohibitively complex to develop and deploy. Now malicious actors can readily and easily purchase powerful capabilities at an increasingly low cost.

This growing marketplace of more affordable, accessible, and advanced commercial cyber tools, including commercial spyware, is already changing the cyber landscape – making it harder for the international community to hold parties accountable for bad behavior, and introducing new instability to cyberspace.

And then there's AI, which has the potential to help malicious cyber actors circumvent our defenses and cover their tracks.

Clearly, we have reached an inflection point when it comes to cyber security. But for all of the challenges of cyber technology, to our individual institutions and infrastructure, and to peace and security more broadly, there is also massive potential for increased collaboration to combat these threats.

The United States is working with likeminded countries to highlight and condemn disruptive, destructive, and destabilizing behavior in cyberspace, including that of the DPRK.

But more than that, we're working to stop this behavior in its tracks.

This includes the International Counter Ransomware Initiative, which the United States founded alongside our partners in 2021. This initiative is helping us build collective resilience to the ransomware through shared policy approaches and information sharing.

It includes supporting efforts like that of the United Kingdom and France, who have initiated the Pall Mall process to address the proliferation of commercial cyber tools.

It includes engaging with the private sector, civil society, and international partners to shape the parameters around AI, so it is used to help defend against cyberattacks, rather than enable them.

Because we know that when used properly, AI can synthesize lessons learned across disparate incidents and geographies; it can help us learn and enact policy changes as we scale up in near real time; and it can enable us to write less vulnerable software in the first place.

We also must continue to work in the GA, where we have heard the call, from 161 states to institutionalize conversations from the Open-Ended Working group on security and use of ICTs and create a permanent, action-oriented Program of Action within First Committee. Because they understand the role the UN can play in leveraging technology to keep our institutions safe, and advancing a human rights-based and multistakeholder approach to the governance of digital technologies.

Finally, we must, must prioritize this work here in the Security Council, and commit to ensuring this important conversation is not the last.

So, let us work together to protect our most critical infrastructure from attacks, and to protect all of us, who rely on it from harm.

Thank you, and I will now resume my role as co-chair.

III. Security Council Members

Slovenia

Thank you very much, Madam Chair.

I extend my gratitude to the Republic of Korea, the United States, and Japan for hosting today's Arria-formula meeting.

I would also like to thank the briefers of today, Mr. Ebo, Dr Geiss, and Ms. Kennedy. Thank you very much for your insightful briefings.

Madam Chair,

Allow me to address two points pertinent to the topic of today's meeting.

First, on the emerging trends of malicious activities in cyberspace.

It is our view that having an accurate understanding of the cyber threat landscape is paramount for a discussion about cooperative measures that the international community can take in response to malicious cyber activities.

In this respect, we commend the ongoing work of the dedicated UN Open-ended Working Group.

At the same time, it is important to highlight that the cyber threat landscape is constantly evolving.

For instance, use of ransomware, along with threats to critical infrastructure vital for civilian life, among others, can now be seen as posing additional challenges to international peace and security, and as such it deserves the attention of the Security Council.

Of further importance are threats to democracy manifested in manipulation of democratic processes. This is especially critical in the "super election year" 2024 when almost half of the world population will go to the polls.

Simultaneously, Artificial Intelligence is acting as a potential accelerator of all threats in the cyber domain. It possesses the capability to broaden the accessibility of advanced cyber tools and techniques, thereby extending their reach to a broader

spectrum of both State and non-State actors. As such, it deserves special attention and enhanced international cooperation.

Secondly, Madam Chair,

Regarding the role of the Security Council in addressing cyber threats.

The Council bears the primary responsibility for the maintenance of international peace and security.

To fulfil its responsibility, the Council should engage in the consideration of cyber threats to peace.

Malicious cyber activities, such as those that generate revenue supporting the proliferation of weapons of mass destruction or those that target critical civilian infrastructure, including satellite networks, have the potential to endanger the security of citizens and thus pose a threat to international peace and security.

Given their cross-border nature, addressing such threats necessitates multilateral cooperation.

In our view, the Council should address incidents in which malicious cyber activities exacerbate conflict, just as the Council would have reacted to threats posed by conventional means. Similarly, it should address activities that incite violence against civilian populations, cause humanitarian suffering, or affect the work of humanitarian organizations.

In an era marked by the growing digitalization of conflicts, it is crucial to emphasize that international law, in particular the Charter of the UN, as well as International humanitarian and human rights law, is applicable to cyberspace and must be respected.

Madam Chair,

Allow me to conclude by assuring you of our unwavering commitment to collaborate with the Council members and the broader UN membership in continuing discussions on cyber threats that are of shared concern to international peace and security. Thank you.

Switzerland

Madam President,

I would like to thank the Republic of Korea for organizing this important debate. I would also like to thank the speakers, Mr Adedeji Ebo, Mr Robin Geiss, and Ms Valeria Kennedy, from Chainalysis Inc, for their detailed contributions. The diplomats in this room have a lot to learn from you.

Recent years have seen some worrying developments in cyberspace. We have already discussed the challenges of cybersecurity within this Council last May. It is also important to address the specific dimension that the speakers have just described, in which states threaten international peace and security by resorting to means of cybercriminals. This threat affects us in many ways. Money, such as cryptocurrencies, and data are stolen or extorted, and critical infrastructures such as energy supplies and healthcare systems are paralyzed. This threat also affects us when funds obtained in this way are used for purposes that violate international law and the resolutions of this Council.

International law applies in cyberspace. It applies to all States and also includes existing obligations of due diligence. These require states to take reasonable and necessary measures to prevent the activities of non-state actors on their territory that violate the rights of other States.

It is also clear that the sanctions measures decided by this Council must be fully implemented in all areas, including cyberspace.

As an international community, we are not powerless in the face of this malicious behavior. The Financial Action Task Force on Money Laundering (FATF) has set international standards to combat money laundering and the financing of terrorism and proliferation. It is up to governments to implement these recommendations. But in an area as interconnected as cyberspace, the private sector also has an important preventive role to play. The Geneva Manual - managed by the DiploFoundation - provides guidance on how standards of responsible behavior in cyberspace can be implemented by non-state actors.

The implementation of the "UN norms of responsible State behavior in cyberspace" is a key element in identifying and addressing existing and emerging threats to peace and security. I would also like to emphasize the importance of the work of the "Open-

ended Working Group on Developments in the Field of Information and Telecommunications" and the development of the "Programme of Action to advance responsible State behavior in the use of ICTs in the context of international security ", which will pave the way for future action in this area. The Security Council – and this was mentioned - also has a role to play. It can send out a strong signal by promoting respect for international law and the norms of responsible State behavior in cyberspace, and by taking account of the realities and threats in cyberspace in its work - for example with regard to sanctions. The 1718 Committee's panel of experts on DPRK is a good example of how important information can be gathered and analyzed on malicious activities in cyberspace in violation of sanctions. It is therefore all the more regrettable that its mandate was not extended last week because of a veto.

Madam President,

Despite the risks, new technologies and cyberspace also represent opportunities to meet the challenges of tomorrow. In his New Agenda for Peace, the Secretary-General encourages us to find new ways of protecting ourselves against these new threats. In addition, the negotiations on the Pact for the Future offer us the opportunity to develop a common understanding, notably in the area of cybersecurity, to strengthen trust and to make progress towards a lasting peace.

I thank you.

Ecuador

- Agradecemos a los expositores.

- Felicitamos a Corea la convocatoria a esta reunión que enfoca el complejo escenario que enfrenta el mundo frente a la continua evolución de las tecnologías de la información y de las comunicaciones (TICs), incluidas las tecnologías emergentes.

- Ecuador considera que si bien las TICs, facilitan procesos más eficientes que contribuyen al desarrollo, también pueden representar crecientes amenazas como ciberataques que ponen en riesgo a la población civil y a la infraestructura critica a nivel global, constituyéndose claramente, en una de las amenazas más graves a la paz y a la seguridad internacionales.

- Las oportunidades que ofrecen las nuevas tecnologías para proteger mejor nuestras poblaciones y salvar vidas, deben ir acompañadas de sistemas que prevengan que el desarrollo y la digitalización, puedan ser usados para promover el odio y la desinformación, capaces de alentar el extremismo y exacerbar los conflictos.

- El Ecuador rechaza la militarización y el emplazamiento de armas en el ciberespacio, por lo que le preocupan sustancialmente los riesgos que suponen las armas autónomas letales, y la necesidad de que todos los sistemas de armamento respondan a un control humano significativo, bajo el único marco viable como es el de la responsabilidad y la rendición de cuentas

- En esa línea, Ecuador reitera su condena a los ciberataques y a todo uso malicioso de la tecnología, toda vez que su naturaleza criminal e injustificable socava los esfuerzos mundiales hacia el uso pacífico del ciberespacio.

- Asimismo, mi delegación destaca que las crecientes ciberamenazas continúan impactando de manera desproporcionada a mujeres y niñas, por lo que es prioritario la incorporación de una perspectiva de género en este ámbito.

- Mi delegación valora y apoya las discusiones del Grupo de Trabajo de Composición Abierta sobre la seguridad y uso de la información y las comunicaciones, en el

contexto de la seguridad internacional, y destaca, asimismo, que estas discusiones permiten seguir avanzando en el análisis y construcción de mecanismos en la materia.

- Así mismo celebramos los avances tangibles como la creación de un Directorio Global de Puntos de Contacto, que se configura como una medida efectiva de fomento de la confianza, que puede contribuir a promover un entorno de TICs abierto, seguro, estable, accesible y pacífico.

- Destacamos la importancia del aprovechamiento de las tecnologías emergentes, como la inteligencia artificial, en estricto apego al derecho internacional, los derechos humanos y el derecho internacional humanitario. Considerándola una herramienta con que se puede contribuir a los esfuerzos de mantenimiento y consolidación de la paz, su uso correcto, y la necesidad de acordar un marco mundial que regule y refuerce los mecanismos de supervisión del uso de la tecnología con fines antiterroristas, es primordial.

- Ecuador está convencido de que la cooperación internacional y la construcción de capacidades, son herramientas fundamentales y efectivas para promover un entendimiento común en la materia, hacer frente a las ciberamenazas y superar las asimetrías existentes que permitan un comportamiento responsable de los Estados. Para ello la contribución que las organizaciones regionales pueden brindar para el desarrollo de capacidades y para la implementación de las referidas normas. Destaco por ejemplo la valiosa labor de la Organización de Estados Americanos en este ámbito, en particular en los esfuerzos contra el ciberdelito y el terrorismo.

- Nuestra responsabilidad es promover y aprovechar el desarrollo tecnológico como un facilitador de la paz, y como una herramienta más de protección de la población civil. Es fundamental que exista un compromiso mundial frente al uso responsable de las tecnologías de la información y la comunicación como clave para garantizar un uso pacífico del ciberespacio. Por ello consideramos que el Consejo de Seguridad debe seguir promoviendo mecanismos efectivos para la reducción de la vulnerabilidad de la infraestructura crítica, así como el fortalecimiento del uso de las tecnologías como medios para la consolidación de la paz.

France

Madame la Présidente,

Les implications des menaces cyber pour la paix et la sécurité internationales ne sont plus à démontrer. Nous le savons, des cyberattaques contre des infrastructures critiques peuvent produire des effets d'une extrême gravité, en période de paix comme de conflit armé. Mais le paysage des menaces cyber ne cesse de se recomposer, ce qui justifie une attention soutenue.

Nous observons notamment une croissance continue des activités d'espionnage stratégique et industriel. En 2023, les autorités françaises ont aussi constaté une hausse de 30 % des attaques par rançongiciels, pouvant viser des secteurs essentiels comme la santé et l'énergie. L'impact des attaques menées contre certains Etats en 2022 illustre le potentiel déstabilisateur des rançongiciels pour le fonctionnement des institutions d'un Etat. Les rançongiciels, ainsi que les vols de cryptomonnaies, peuvent également être utilisés par des Etats pour financer la poursuite de programmes illégaux d'armes de destruction massive.

Ces menaces cyber sont démultipliées par la diffusion non contrôlée et l'usage irresponsable d'outils et de services d'intrusion disponibles sur le marché. Cette tendance, aujourd'hui à la hausse, comporte des risques pour la protection des droits fondamentaux, la sécurité des Etats voire pour la stabilité internationale.

Madame la Présidente,

Pour répondre à ces menaces en constante évolution, le Conseil de Sécurité et l'ensemble du système des Nations unies doivent maintenir leur mobilisation.
Le Conseil de sécurité doit continuer d'intégrer la dimension cyber dans ses travaux. Il doit par exemple prendre en compte l'usage de procédés cybercriminels à des fins de prolifération ou de contournement des mesures imposées par ses résolutions. Le dernier rapport annuel du groupe d'experts du Comité 1718 illustre ainsi l'importance croissante des activités cyber malveillantes dans le financement des programmes balistiques et nucléaires de la Corée du nord. Nous ne pouvons à cet égard que déplorer que la Russie ait empêché la reconduction du groupe d'experts du Comité 1718, dont les travaux sont une source d'information précieuse.

En outre, nous devons promouvoir et soutenir les normes et cadres juridiques qui concourent à la stabilité du cyberespace et à la lutte contre la cybercriminalité. La France continue de s'engager dans les travaux pertinents de l'Assemblée générale à cette fin.

En 1ère Commission, elle soutient les discussions qui visent à approfondir des compréhensions communes du cadre normatif consensuel de comportement étatique responsable. A ce titre, elle continue de promouvoir la proposition transrégionale d'un mécanisme permanent et inclusif de Programme d'action pour appuyer les Etats dans la mise en œuvre de ce cadre. En 3e Commission, la France demeure investie pour faire aboutir cet été les négociations de la future convention de lutte contre la cybercriminalité des Nations Unies, qui devra favoriser une coopération internationale robuste et efficace, tout en garantissant le respect des droits et des libertés fondamentales.

La France, en outre, souhaite favoriser la coopération multi-acteurs contre la prolifération et l'usage irresponsable des capacités de cyber-intrusion disponibles sur le marché. Elle entend continuer de promouvoir, avec le Royaume-Uni, le processus de Pall Mall, qui vise à alimenter les discussions sur les réponses à apporter à ce phénomène.

Je vous remercie.

Algeria

Mr. Chair,

Thank you for convening this important Arria-formula meeting on the growing dangers of cyber threats to global security.

Our gratitude goes also to Mr. Adedeji, Dr. Robin Geiss, and Ms. Valeria Kennedy, for their invaluable insights.

This meeting highlights the alarming rise in malicious cyber activity. From ransomware attacks on critical infrastructure to the theft of digital assets and data, these acts endanger public safety and political stability. The involvement of state and non-state actors further complicates this landscape.

The spread of disinformation online fuels divisions, terrorism and intolerance. The experience of COVID-19 pandemic has shown indications of this trend, with false information interfering in state affairs, hampering cooperation, and threatening Peace.

In light of these realities, I wish to highlight the following key points:

First, the UN Charter's principles, including non-use of force, respect for sovereignty, non-intervention, and peaceful dispute resolution, apply equally to Cyberspace.

Second, we reaffirm our dedication to an open and secure cyberspace, vital to achieving global development goals. A legally binding framework is needed to ensure stability and responsible behavior by state actors.

Third, we must help developing countries build resilience to cyber threats and bridge the digital divide. Capacity building is essential for securing cyberspace for all nations.

Fourth, the international community must combat the spread of disinformation online. Governments and stakeholders must work together, in line with international law, to counter this challenge through sustained effort and cooperation.

Thank you.

The United Kingdom of Great Britain and Northern Ireland

I join others in thanking the Republic of Korea, Japan and the US for organising this discussion and to the briefers for highlighting so clearly how cyber threats are impacting peace and security.

We want to address three issues of particular importance to the UK:

Firstly, ransomware poses an acute threat, not least to our critical national infrastructure. It can disrupt vital public services and undermine confidence in the integrity, reliability and safety of our networked economies. The way ransomware operates is obviously borderless and with cybercriminals often based in uncooperative jurisdictions, an international response is needed to constrict the ecosystem that facilitates it. Whilst criminal use of ransomware is the most significant threat in terms of volume, the most advanced threats to UK critical national infrastructure still come from states and state-aligned groups.

Secondly, the growing market of commercial cyber capabilities is transforming the cyber threat landscape. Such tools and services increase the range of actors with access to advanced and difficult to attribute hacking capabilities, creating potential for increased instability in cyberspace. The recent case of iSoon shows that ‘hackers for hire' and spyware capabilities are already being used irresponsibly by states.

The Pall Mall Process – an international multi-stakeholder initiative launched by the UK and France earlier this year – is considering policy options and new practices to address this shared threat.

Thirdly, whilst cryptocurrency provides a fast and anonymous means of transferring funds globally, this anonymity can also facilitate malicious cyber. Whilst most are legitimate, some exchanges and services are criminally complicit in exchanging funds for other forms of currency or mixing transactions to prevent tracing. These are exploited not only by cyber criminals, but other actors seeking to obscure the origin or destination of funds, including some nation states, state-aligned actors and terrorists.

We are, for example, very concerned by DPRK’s use of malicious cyber activities to obtain cryptocurrencies to fund their illegal WMD programme.

President, the international community already has important tools that are applicable to these emerging threats, such as the UN Norms of Responsible State Behaviour agreed by consensus in the General Assembly. We urge all states to uphold these commitments. The UK remains committed to doing so and to supporting others through cyber capacity building and enabling public private partnerships.

Sierra Leone

Chair,

1. I thank the co-hosts for holding this Arria Formular meeting.

2. Let me also thank **Adedeji Ebo, Deputy to the High Representative for Disarmament Affairs, Robin Geis,** Director of the UN Institute for Disarmament Research (UNIDIR), and **Valerie Kennedy,** Director of Intelligence Solutions for Investigations and Special Programmes at Chainalysis.

3. As the threat landscape in cyberspace continues to evolve and pose significant challenges to global stability, it is imperative that we engage in deepened exchanges to enhance our collective understanding and response to these evolving security challenges. Addressing emerging trends that pose additional challenges to global stability requires a unified and proactive approach by the international community.

4. Sierra Leone acknowledges the significant efforts of the Security Council in addressing emerging threats to international peace and security, including the recent debates on cybersecurity and the increasing focus on the nexus between information and communication technologies (ICT) and global security. We commend Estonia for convening the first open debate on cybersecurity during its Presidency in June 2021 and recognize the valuable discussions held in various Arria-Formula meetings on this critical issue.

5. Despite differing views on the Council's mandate in this area, Sierra Leone emphasizes the necessity of effective coordination and cooperation to combat cyber threats comprehensively.

6. The evolving threat landscape, characterized by the proliferation of malware, ransomware attacks, cryptocurrency heists, and the expansion of malicious actors, poses significant risks to international peace. The recent escalation in the frequency and scope of ransomware attacks, targeting critical infrastructure and essential public services, demonstrates the severe impact of cyber threats on public safety and political stability and requires continuous vigilance. Sierra Leone is also deeply concerned about the implications of cyber threats, including the use of cybercrimes to fund illicit activities and evade international sanctions. All of these underscores

the urgent need for enhanced international cooperation and capacity-building efforts to combat these threats effectively.

7. In this regard, Sierra Leone enacted a Cybersecurity and Crime Act, in 2021, developed to comply with ECOWAS Directives, the Malabo Convention and the Budapest Convention. It provides the necessary legal framework required to facilitate the investigation of cybercrimes and cyber-related crimes, clearly identifies the penal offences, and enables effective and efficient international cooperation to exchange digital evidence.

8. Sierra Leone further emphasizes the interconnected nature of cybersecurity threats, which transcend borders and affect all states, irrespective of their technological capacities. We recognize the importance of inclusive discussions on the threat landscape to promote international cooperation and capacity-building efforts that are essential to address the multifaceted nature of cyber threats effectively.

9. In light of the current challenges posed by malicious activities in cyberspace, Sierra Leone presents the following recommendations to combat the threats to cybersecurity and uphold international peace and security:

10. *Firstly*, enhance awareness and understanding of emerging cyber threats, such as ransomware, crypto-heists, and financial crimes, through evidence-based research and horizon scanning.

11. *Secondly*, strengthen the normative framework for responsible State behavior in cyberspace and promote adherence to international law in cyberspace to prevent and mitigate malicious cyber activities. Sierra Leone therefore welcomes and considers the adoption of universal instrument, such as a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, to tackle Cybercrime as not only an imperative but also fundamental to the maintenance of international peace and security.

12. *Thirdly*, support capacity-building efforts to enhance States' abilities to prevent, mitigate, and respond to cyber incidents, particularly in less developed countries with limited technological capacities. *Fourthly*, Foster international cooperation and

information sharing to counter cyber threats effectively, including through the establishment of platforms and frameworks for collaborative action.

13. Sierra Leone is of the view that the UN Security Council can play a pivotal role in addressing evolving nature of cyber threats and promoting international peace and security through comprehensive engagement with relevant UN General Assembly Committees and Specialized Agencies.

14. We urge all member States to prioritize cybersecurity as a critical component of their national security strategies and emphasizes the need for a coordinated, multilateral approach to address the growing challenges in cyberspace. The collective measures proposed are essential to counter the evolving threats posed by cybercriminals and safeguard the integrity of the digital realm.

15. In **conclusion**, Sierra Leone reaffirms its commitment to promoting cybersecurity as a fundamental aspect of international peace and security and working collaboratively within the Security Council and the broader international community to address the complex and evolving threats to cybersecurity. By enhancing our understanding of the threat landscape, strengthening normative frameworks, and promoting international cooperation, we can effectively combat cyber threats and uphold international peace and security in the digital age.

16. I thank you.

The People's Republic of China

主席先生:

感谢埃博和盖斯代表联合国裁军厅、裁研所所作通报。

当前信息技术革命日新月异,数字经济蓬勃发展,极大促进各国经济社会发展和人类文明进步。与此同时,网络攻击和犯罪大幅增长,网络恐怖主义成为全球公害,网络军事化趋势加剧,关键基础设施安全风险有增无减,国家和地区间数字鸿沟不断扩大。为因应上述风险挑战,中方主张:

一是要强化网络空间国际规则制定。制定各方广泛参与、普遍接受的网络空间国际规则,是维护网络空间长治久安的关键。各国应根据网络空间的独特属性和形势发展需要,坚持责任共担、权利共享原则,履行网络空间负责任国家行为框架,并在联合国主持下讨论现有国际法适用及制定新的国际法律文书问题,争取达成更多共识。中国提出的《全球数据安全倡议》为推进网络安全治理提供了有效解决方案,可作为各方未来讨论的基础。

二是要防止网络空间成为新的战场。网络军事化和网络战是网络安全的重大威胁。国际社会应遵守《联合国宪章》宗旨和原则,维护网络空间和平属性,不从事危害他国安全的网络活动,通过对话与合作解决网络安全威胁。各方应审慎对待武装冲突法适用于网络空间问题,防范网络军备竞赛。

三是要以专业、负责任的态度开展网络攻击溯源。网络空间因其虚拟属性,在有效溯源方面存在诸多困难。可被证实的溯源是应对网络攻击的前提,也是讨论各国责任和义务的基础。无端散布虚假消息、恶意抹黑,甚至贸然给他国"定罪",只会加剧对抗,影响国际社会合作解决网络安全挑战的努力。

四是要推进网络安全能力建设国际合作与援助。维护网络安全是全球性课题,没有哪个国家能置身之外、独自应对。各国应在自愿基础上,开展政策交流、技术交流、信息共享及立法执法领域的合作,共同应对信息技术滥用,防范网络攻击,打击网络恐怖主义和网络犯罪,提升网络安全保障能力,同时不应以向他国提供网络安全援助为由,对受援国或第三国实施恶意网络行为。中国支持向广大发展中国家提供网络安全能力建设援助,反对对发展中国家和平利用科技施加不合理限制。

主席先生,

网络空间的风险挑战层出不穷,国际社会应坚持多边主义,坚守公平正义,兼顾安全与发展,深化对话与合作,共同推动网络安全治理和国际规则制定。安理会作为维护国际和平与安全的首要机构,也应为此发挥积极作用,包括支持联合国框架下关于制定网络空间国际规则的讨论、促进打击网络恐怖主义国际合作、鼓励会员国加强网络安全能力交流与合作等,从而推动构建和平、安全、开放、合作、有序的网络空间。中方也愿继续与各方一道,以团结合作凝聚最大公约数,携手构建网络空间命运共同体。

谢谢主席。

Guyana

I thank the Republic of Korea, Japan, and the United States for convening this Arria-Formula Meeting on Cyber Security. I also wish to thank Mr. Ebo, Dr. Geiss, and Ms. Kennedy for their briefings.

Excellencies, Colleagues,

Cyberspace forms part of our everyday life and plays an essential role in our countries' social and economic development. However, the rapid advancement of technology has brought with it surges in cyberthreats, cyberattacks and cybercrimes with implications for the maintenance of international peace and security. Cybersecurity is, therefore, a major issue that must be addressed, as we seek to create an open and secure cyberspace.

In recent years, we have witnessed a growth in criminal activities within cyberspace, including by non-State actors. Such activities range from the hacking of Government websites and attacks on critical information infrastructure to spreading of misinformation and incitement of violence, online exploitation, and the illicit use of cryptocurrencies. An open cyberspace is also creating opportunities for terrorist organisations to divert finances to fund their activities, plan attacks and recruit and train persons to join their networks.

These activities have exposed significant cybersecurity vulnerabilities in both developed and developing countries, more-so in the case of the latter. In these circumstances, attention to and investment in strengthening cyber capabilities and cyber resilience at the national, regional, and international levels are critical.

Focus should also be placed on bolstering cybersecurity to address criminal activities in cyberspace and its associated risks and vulnerabilities. To this end, there must be increased efforts to promote public awareness, robust regional and international cooperation, capacity building initiatives and public-private partnerships. There is also a need to establish international technical standards and legislative frameworks to govern the safe use of cyberspace.

Nationally, Guyana has been undertaking some of these initiatives, which include training in the public sector to raise cybersecurity awareness and on protecting digital information and the modernisation of our Cybercrime Act. At the global level, Guyana recognises and has been participating in the processes within the UN system that are dedicated to addressing cyber issues, including the Open-ended Working Group on security of and in the use of information and communications technologies (ICTs) and

the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Given the evolving cyberthreat landscape, regional and international cooperation in cybersecurity is of paramount importance.

The Security Council, in fulfilling its mandate of maintaining international peace and security, must be a part of the dialogue on cybersecurity, and explore ways of preventing and addressing conflicts arising from or being exacerbated by cyber threats and attacks.

In conclusion, co-Chairs, Guyana wishes to underscore the importance of continuing discussions and engagements on cybersecurity towards advancing a global response to ongoing and future cyberthreats.

I thank you.

Mozambique

Excellencies,
Co-Chairs,

1. Mozambique thanks the Permanent Missions of Korea, Japan and the United States of America for organizing this important Arria Formula.

2. We also thank the briefers for their valuable insights on the topic and their comprehensive assessment of the situation at hand.

Co-Chairs,

3. As we highlighted during the Arria Formula meeting on the issue last May, the cyber threat landscape has become increasingly complex and concerning. Threat actors are employing sophisticated tactics to exploit vulnerabilities in various sectors. This reality compels us to remain vigilant and adopt robust cybersecurity measures to mitigate these evolving threats.

4. As digital technologies become omnipresent, accelerated by the pandemic and driven by advancements, such as artificial general intelligence, we face increased state-sponsored attacks, a surge in cyber espionage, and cybercrime.

5. These developments demand robust cybersecurity at individual, national and international levels.

Co-chairs,

6. I will try to focus on three points from the perspective of the Global South:

First:

7. The vast disparities in cyber resilience between regions, with Africa and Latin America straggling on cyber defense capabilities, in contrast to North America and Europe, constitute a serious gap and pose a major threat to international peace and security.

8. No state can afford to be eternally trapped under the so called “cybersecurity poverty line” due to factors like costs, skills gaps and access challenges. We, therefore, must urgently address this line, by helping states and organizations in the Global South.

Second:

9. Technological risks, such as disinformation/misinformation, enabled by deepfakes and AI-powered phishing could be weaponized to disrupt elections, incite war, and radicalize public opinion and incite extremism.

10. With the proliferation of new technologies, such as generative AI and their increasingly widespread use by cyber adversaries, extremists, and radicals, safeguarding the integrity and fairness of electoral processes and public discourse becomes an issue of international peace and security.

Third:

11. Data is the “new oil”!

12. The weaponization of data is a critical concern, especially when it comes to vulnerable populations. Safeguarding vulnerable populations’ data and ensuring responsible AI use are vital for global security and ethical progress.

Co-Chairs!

13. Tackling these and other challenges requires a multi-faceted approach:

- Governments should focus on crafting robust cyber legislation and fostering international cooperation. In this context, the recently unanimously adopted General Assembly Resolution *“Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development”* is, indeed, a welcome collective approach and a step in the right direction.

- Businesses, integrating cybersecurity across operations and adopting the “Zero Trust” security model is imperative.

- Public cyber hygiene education developing cybersecurity capacities in the Global South are crucial steps in mitigating future risks.

- Public-private partnerships also play a vital role in enhancing national cybersecurity resilience.

14. Recognizing the vital significance of digital resilience in our increasingly interconnected world, Mozambique has undertaken significant steps in this direction:

- We have ratified the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention), which serves as a legal framework designed to harmonize data protection and privacy laws across Africa.

- Mozambique has also enacted Law 03/2017 on Electronics Transactions governing electronic transactions within the country, as well as Decree 59/2019, which established the Digital Certification System of Mozambique, enhancing digital security and authentication.

- We also have been actively participating in regional and international forums in the fight against cybercrime.

15. As we navigate the ever-changing domain of cybersecurity, close cooperation between governments, businesses, individuals and amplifying Global South voices is imperative to bolster our collective digital defenses and secure international peace.

16. To conclude, Mr. Chair, Mozambique remains committed to engaging and unifying efforts to boost cyber resilience globally.

I thank you.

The Russian Federation

Г-н Председатель,

Благодарим заместителя Высокого представителя по вопросам разоружения Адедежи Эбо и директора Института ООН по исследованию проблем разоружения Робина Гайса за их доклады. Внимательно выслушали представителя частного сектора Валерию Кеннеди.

Российская Федерация стояла у истоков обсуждения вопросов международной информационной безопасности в ООН. Впервые мы подняли эту тему в Генассамблее еще в 1998 году. 26 лет назад Россия внесла первый проект резолюции по данной теме, впоследствии ставший ежегодным. По российской инициативе вопросы безопасности в сфере использования информационно-коммуникационных технологий обсуждались сначала в рамках профильной Группы правительственных экспертов (ГПЭ) ООН, а после – в инклюзивном формате Рабочей группы ООН открытого состава, которая сегодня работает под умелым председательством Постоянного представителя Сингапура Бурхана Гафура.

Именно РГОС является уникальной единой переговорной площадкой под эгидой ООН для обсуждения вопросов международной информационной безопасности. В ее рамках все государства-члены могут на равных участвовать в дискуссии и принятии консенсусных решений по различным аспектам ее мандата.

На этом фоне нам неясна «добавленная стоимость» обсуждения проблематики международной информационной безопасности на площадке Совета Безопасности. Считаем контрпродуктивным дублирование усилий международного сообщества и «растаскивание» данной темы по различным ооновским трекам. Большой вопрос, который по сей день остается нерешенным, какие случаи злонамеренного использования информационно-коммуникационных технологий (ИКТ) можно было бы с уверенностью отнести к прямым угрозам международному миру и безопасности.

Убеждены, что усилия международного сообщества должны быть сосредоточены на продолжении укрепления межгосударственного взаимодействия в рамках РГОС в целях достижения конкретных, практических результатов в деле обеспечения международной информационной безопасности. Приветствуем согласование инициативы о формировании глобального межправительственного реестра в этой области на основе идеи, предложенной Российской Федерации. Считаем принципиально важным закреплять и развивать достигнутые РГОС результаты, в том числе в рамках будущего

переговорного формата, решение о котором должно быть также принято в рамках РГОС. Россия уже представила свое видение постоянно действующего инклюзивного механизма в данной области.

Для нашей страны приоритетом является формирование универсальных юридически обязывающих инструментов в области информационной безопасности, что будет способствовать предотвращению межгосударственных конфликтов в этой сфере. В 2023 г. Россия представила в Генассамблее ООН прообраз профильного международного договора – концепцию конвенции об обеспечении международной информационной безопасности. Приглашаем все государства-члены к предметной дискуссии на основе нашего предложения.

Г-жа Председатель,

Вызывают самую серьезную озабоченность попытки западных коллег и их союзников использовать обвинения в злонамеренной деятельности с использованием ИКТ в качестве рычага давления на «неугодные» государства, включая КНДР. Сколь-нибудь убедительных доказательств в подтверждение этих слов не приводится.

Инструментом в этой нечистоплотной игре неоднократно становилась Группа экспертов Комитета СБ ООН 1718 по КНДР, которая по наводке одного государства обращалась к российской стороне по поводу приписываемых Пхеньяну компьютерных атак на российские структуры. Когда же мы запросили точные данные, необходимые для расследования предполагаемых инцидентов, – такие как точное время, использовавшиеся IP-адреса, серверные мощности, компьютерное оборудование и координаты его местоположения – эксперты отвечали, что не получали от своего «источника» дополнительную информацию.

Уважаемые коллеги,

Это наглядная иллюстрация того, что эта Группа экспертов, которую так превозносят ряд коллег, не справлялась со своими обязанностями и, по сути, занималась сбором и перепечаткой низкопробных, политически ангажированных слухов из сомнительных источников. Например, на фоне существенной эскалации на Корейском полуострове из-за наращивания США и их союзниками по НАТО военной активности, Группа экспертов анализировала такой крайне «важный» с точки зрения поддержания международного мира и безопасности вопрос по газетным заголовкам, как происхождение дамских сумочек. Сегодня нам предлагается принять выкладки данной Группы в области безопасности ИКТ как истину в последней инстанции. Это несерьёзно.

Мы неоднократно разъясняли нашу позицию по продлению мандата Группы экспертов и в целом в отношении необходимости серьезной дискуссии

по северокорейскому санкционному режиму. К сожалению, западные коллеги подтвердили свою неготовность к обсуждению реальных шагов по справедливому урегулированию ситуации на Корейском полуострове.

Категорически отвергаем любые рассуждения на тему того, что Россия якобы поощряет злонамеренные действия в информационном пространстве. Это просто абсурд. Россия на протяжении четверти века выступает за предотвращение милитаризации информационного пространства. Мы начали это делать задолго до того, как страны Запада вообще признали существование такого риска. Именно Россия все эти годы предлагала заключить юридически обязывающие договоренности в целях предотвращения конфликтов в этой сфере. Западные же страны, прежде всего США, эту идею как отвергали, так и продолжают отвергать, стремясь сохранить за собой максимальную «свободу рук».

Лицемерие западных коллег особенно проявляется на фоне признания высокопоставленными лицами США фактов проведения против России наступательных операций с использованием ИКТ, а также закрепления в доктринальных установках Вашингтона и НАТО «наступательных» – а по сути агрессивных – подходов.

Односторонние и бездоказательные инсинуации в «агрессивных» и «враждебных» действиях в адрес государств в информационном пространстве неприемлемы. Атрибуция ответственности, как заметили сегодня наши китайские коллеги, требует профессионального подхода и предоставления исчерпывающих технических доказательств – такое понимание было впервые закреплено в докладе профильной ГПЭ в 2013 году. Этого невозможно добиться без деанонимизации информационного пространства, а также формирования справедливых и прозрачных механизмов установления источников компьютерных атак. Однако этому препятствуют прежде всего разработчики ИКТ западных стран, прикрываясь предлогами о защите свободы слова. При этом, эта самая свобода ограничивается или попросту нарушается их же компетентными ведомствами в сочетании с организацией американскими властями глобальных программ «кибершпионажа» и манипулирования информационными потоками через использование потенциала ИТ-корпораций. Как бы ни хотелось нашим американским коллегам стереть из общественной памяти разоблачения Эдварда Сноудена, мир их прекрасно помнит.

Не стоит забывать и о том, что США и их союзники в свое время сопротивлялись созданию профильной РГОС, а после попросту принялись «ставить ей палки в колеса», продвигая идеи создания конкурирующих переговорных площадок, где западные страны играли бы «первую скрипку» –

таких, как «Программа действий по поощрению ответственного поведения государств».

Тревожат и попытки размывания глобальной дискуссии по вопросам противодействия использованию ИКТ в преступных целях. Ярким примером является упоминавшаяся сегодня «инициатива по противодействию вирусам-вымогателям». Подобные «клубы для избранных», не особо скрывающие свою политизированную направленность, подрывают усилия государств-членов ООН по разработке универсальных механизмов борьбы с использованием ИКТ в преступных целях – в частности, по линии профильного Спецкомитета ООН.

Уважаемые коллеги,

Российская Федерация занимает конструктивную позицию в вопросах обсуждения международной информационной безопасности. Наша страна продолжит отстаивать принципы формирования мирной и безопасной ИКТ-среды в глобальном масштабе. Призываем все конструктивно настроенные государства к поддержке этих усилий в рамках РГОС как единой переговорной площадки, в том числе и после окончания мандата действующей Группы в 2025 году.

Благодарю Вас.

Malta

Chair,

I begin by thanking the Republic of Korea, Japan, and US for organising this meeting. I also thank Director Ebo, Director Geiss and Ms Kennedy for their informative briefings.

Today's meeting provides an opportunity to advance the consensual understanding that the UN Charter and international law are applicable to activities in cyberspace. Likewise, it serves to reaffirm the principle of responsible state behaviour in cyberspace, endorsed by the UN General Assembly.

Our efforts to advance international stability in this domain must prioritise the protection and promotion of human rights. In this context, conflict-sensitive and gender-responsive cybersecurity legal and policy reforms are needed.

Malicious cyber activities present multifaceted challenges with profound implications for the maintenance of international peace and security.
Criminal activities in cyberspace have the potential to exacerbate vulnerabilities, disrupt essential services, and escalate conflicts.

Furthermore, high-profile ransomware attacks on government institutions and essential public services can potentially threaten public safety and heighten economic destabilisation and political instability.

We call upon all states to exercise due diligence and take appropriate action against malicious cyber activity originating from their territory. At the same time, strict surveillance, internet shutdowns, and bandwidth throttling are to be condemned as practices that curtail freedom of expression and assembly. Digital platforms are used increasingly to spread dis- and misinformation, hate-speech, misogynistic, homophobic, and radicalising content.

The emergence of quantum computing threatens the cryptographic foundations of secure communication and, thus, the resilience of nations, the stability of critical infrastructure, and the right of citizens to private communication.

State-sponsored malicious cyber actors target financial institutions, including cryptocurrency-related firms. They exploit ransomware and fraudulent techniques to generate illicit revenues.

The DPRK's regime continues to use such illicit revenues, generated by hackers under the Reconnaissance General Bureau, to fund its unlawful WMD programme. Malta condemns these malicious cyber activities in the strongest terms. The 1718 Committee Panel of Experts has played an invaluable role in investigating these crimes and violations. We regret the Council's failure to renew its mandate due to the use of the veto by a permanent member.

The Security Council, together with other relevant UN bodies, should promote an open, secure, stable, accessible, and peaceful cyberspace. It can support capacity-building initiatives for developing nations and promote the development of international legal framework to combat cybercrime, as well as national robust security frameworks to enhance resilience. These measures can also help address the disproportionate impacts that online harms, threats and ICT-facilitated crimes have on women and girls.

Promoting women's leadership and digital literacy in cybersecurity, and engaging women's civil society organisations can accelerate momentum for responding to gendered security challenges in the digital age.

Aside from UN efforts, including through the establishment of a Programme of Action on cybersecurity, the involvement of the private sector is also paramount in fortifying cybersecurity frameworks, in light of its technical expertise and ownership of critical infrastructures.

To conclude, Chair, Malta continues to support discussions in the Security Council on all threats to international peace and security, including in the cyber domain.

I thank you.

IV. Groups

The European Union

Chair,

I have the honour to speak on behalf of the European Union. We very much welcome the opportunity to exchange views on the evolving cyber-threat landscape and its implications for the maintenance of international peace and security.

The Candidate Countries North Macedonia[1*], Montenegro[*], Albania[*], Ukraine, the Republic of Moldova, Bosnia and Herzegovina[*] and Georgia, and the EFTA countries Iceland and Norway, members of the European Economic Area, as well as, Andorra align themselves with this statement.

Colleagues,

In our modern world, cyberspace has become a pillar of all societies, facilitating economic growth and social progress for all citizens.

The EU, like many in this room, however, remains deeply concerned with the parallel increase of malicious activities in cyberspace and the misuse of information and communication technologies. Such activities directly affect citizens' trust in the digital world and increase the risk of escalation and conflict, both in cyberspace and beyond. Such activities can also have adverse effects on the full and effective enjoyment of human rights.

A key trend is the blurring of lines between state-sponsored and criminal or financially motivated actors. We remain particularly concerned that the threat of **ransomware** continues to target private companies and critical sectors such as healthcare. The impact of such ransomware incidents occasionally also rises to the level of a threat to international peace and security.

Where we once focussed primarily on the threat to governments and defence, we now also recognise the real-world impact of irresponsible activity on the broader economy and society. It must be our joint commitment to improve our toolkit for collective

[1*] *North Macedonia, Montenegro, Serbia, Albania and Bosnia and Herzegovina continue to be part of the Stabilisation and Association Process.*

resilience to ransomware and we welcome other delegations sharing their insights and experiences.

In addition, the EU is concerned about the significant threat coming from **state actors that seek political or economic advantage** from coercive action in cyberspace, particularly with regard to critical infrastructure and critical cyber systems.

In this context, the EU and its Member States are alarmed about the number of malicious cyber activities targeting government institutions as well as democratic processes, often with the direct intent to undermine stability and security and to erode trust in the outcome of democratic elections. Recently, the EU joined the United Kingdom and other international partners in expressing serious concerns about the use of cyber operations to interfere with democratic processes and institutions.

Together, we must be prepared to shed light on malicious cyber activity and hold the responsible actors to account. We must continue both to collectively address malign cyber activity, and to enhance **accountability** of actors that conduct themselves contrary to the international obligations and expectations we have all agreed upon, while **fully respecting our international human rights obligations**.

Chair,

The international community recognises that **existing international law, including the UN Charter in its entirety**, is applicable in cyberspace. States have also recognized the applicability of the law of state responsibility, international human rights law, and, in situations of armed conflict, international humanitarian law.

States are increasingly developing **military cyber capabilities**. It is the responsibility of the international community to ensure – should these capabilities be used in armed conflict – that they are used in a manner that complies with longstanding rules of international humanitarian law and in a way that minimizes human suffering.

We urge all States to work towards providing clarity and examples on how existing rules of **International Humanitarian Law** can be applied on cyber operations, especially its fundamental principles of humanity, necessity, proportionality, distinction, and precaution.

Finally, as we confront the threats that concern us most today, we must also look to the future and the implications of **emerging technologies, such as AI**, within the framework for responsible state behavior.

As a concrete and forward-looking measure, the EU supports the **establishment of a Programme of Action on Cybersecurity as a permanent mechanism** in this domain. This initiative seeks to establish a results-based, action-oriented, and transparent mechanism underpinned by inclusive dialogue and cooperation among all relevant stakeholders. This will allow efforts to support states promoting the implementation of the framework for responsible State behavior and capacity building to increase cyber resilience globally.

Chair,

Working together to understand the evolving nature of the threat of malicious cyber activity is crucial to setting the context in which we develop practical measures for international cooperation. We look forward to continue to work with responsible UN member states to identify cyber threats of shared concern to international peace and security and to implement effective measures aimed at decreasing those threats and risks.

Thank you.

Belgium-The Kingdom of Netherlands-Luxembourg (BENELUX)

Thank you, Mr. President,

At the outset, allow me to very much thank the Republic of Korea for organizing this timely Arria-formula meeting with the support of Japan and the United States.

Mr. President,

I would like to deliver this statement on behalf of the Benelux countries, Belgium, Luxembourg and the Kingdom of the Netherlands. The Benelux countries align themselves with the statement made by the EU and would like to underline three additional points:

1.

First, the Benelux countries remain deeply concerned over the increasing and evolving threat of malicious cyber activities. A threat that continues to rise in scale and severity, which may be further exacerbated by emerging technologies, including artificial intelligence.

One trend we observe is the increase of ransomware attacks, the use of ransomware-as-a-service and malicious cyber threats, targeting critical infrastructure, including the health sector and electoral processes. The effects of such incidents could be a growing threat to international peace and security, including where state actors use financial assets obtained from malicious cyber activities.

2.

That brings me to my **second point**: the international community has not been sitting idly by. Under the First Committee of the General Assembly, States developed a cumulative and evolving framework for responsible State behavior. This framework, which has repeatedly been endorsed by the General Assembly, is underpinned by the consensus that international law, in particular the UN Charter, applies in cyberspace. With regards to ransomware, this framework also includes the non-binding norm that states should not knowingly allow their territories to be used for malicious activities.

States have also made important strides to advance cooperation to address cybercrime threats. In this regard, the Benelux countries are parties to the Budapest

Convention and we are actively contributing to the ongoing UN Cybercrime Treaty negotiations.

And there are more ways in which we are playing our part:

- We work with partners to enhance our collective cyber resilience through the EU Global Gateway, the UNODC, Interpol;
- We support multi-stakeholder platforms such as the Global Forum on Cyber Expertise that matches capacity-building needs with resources;
- And we take active part in the Counter Ransomware Initiative, an important partnership that seeks to enhance international cooperation to combat ransomware.

And here, Mr. President, I would like to underline the importance of inclusivity in striving to narrow the digital divide, and considering gender-differentiated impacts of cyber incidents.

3.

Finally, Mr. President, while much is already being done, the Benelux countries are of the view that the Security Council has a vital role in promoting an open, free and secure cyber domain. The Council should continue to address severe malicious cyber incidents. Because as ongoing conflicts demonstrate: the cyber threat is not an isolated threat. It is inherently part of broader threats to international peace and security, the maintenance of which is indeed the primary responsibility of the Security Council.

Mr President, we thank you again for organizing this Arria-formula meeting and we applaud your efforts to raise awareness and address the importance of cyber threats. Thank you.

Canada-Australia-New Zealand (CANZ)

Thank you very much Chair, and may I thank the Republic of Korea, Japan and the United States for bringing us together.

Australia, Canada, and New Zealand welcome the opportunity to discuss the evolving and multifaceted cyber threat landscape in this forum.

Cyber threats can undermine the transformative opportunities otherwise provided by digital technologies. These threats are increasing in scale and sophistication.

Commercial markets for intrusive cyber capabilities are expanding, fuelling proliferation and opportunities for malicious and irresponsible use.

Growing reliance on **Artificial Intelligence** within social, financial and government systems creates an attractive target for cyber threats.

Interference with **democratic institutions** and elections undermines trust in political processes.

Cyber prepositioning on **critical infrastructure** create mistrust and heightens the risk of miscalculation and conflict.

Ransomware represents the most pressing and disruptive cyber threat faced by States.

State-sponsored cybercrime poses a serious risk to international security and global financial systems.

Profits from these criminal enterprises can be used to fund activities that contravene international law, and security frameworks, such as non-proliferation and financial sanctions.

And we have seen the use of ransomware tools to perpetrate financial crimes, including **cryptocurrency theft** which has directly funded weapons programs.

Let me be clear: these behaviours are unacceptable.

States must be unequivocal in their commitment to act in accordance with **international law** and **agreed norms**.

Some argue we need more rules; that cyberspace is a lawless space where malicious actors can act with impunity.

We question the motivations of those perpetrating this myth.

What we need is not more – or new – rules, but adherence to the rules we have already agreed, and greater accountability when they are broken.

We ask the Security Council to affirm the UN agreed framework of responsible State behaviour which, **when implemented and adhered to**, provides a mechanism for promoting an open, secure, stable, accessible and peaceful cyberspace.

As we integrate more technologies into our lives, we become more susceptible to malicious cyber activities, and it is always the most vulnerable that are at higher risk.

We must ensure that cyber security approaches promote gender equality and women's participation and leadership, including through the Women Peace and Security Agenda.

All States must work cooperatively and continue to build cyber resilience to overcome these evolving security challenges.

Thank you.

V. UN Member States

Costa Rica

Señor Presidente,
Agradezco a la República de Corea la organización de esta reunión Arria-formula.

Las actividades maliciosas en el ciberespacio tienen graves consecuencias. No hablo de manera abstracta, sino de nuestra experiencia concreta. Costa Rica fue víctima de dos importantes ataques de ransomware en 2022. Un ataque contra 27 de nuestras estatales y otro contra nuestro sistema de salud. Esto condujo a repercusiones sin precedentes en nuestra economía, en la atención de la salud y en otros sectores críticos del Estado, como nuestro sistema de seguridad social.

Declaramos un estado de emergencia y solicitamos la asistencia de Estados y líderes no gubernamentales en la arena digital. Los grupos que llevaron a cabo estos ataques los anunciaron públicamente, y el Estado desde donde realizaron sus operaciones es conocido.

Nuestra recuperación no ocurrió de un solo golpe. Fue un proceso largo, costoso y doloroso debido a la encriptación de los datos de nuestro Estado y de nuestros ciudadanos. Sabemos que no estamos solos en nuestra experiencia, pero algunos optan por aceptar silenciosamente las exigencias de los hackers en lugar de hablar sobre su experiencia. Estos incidentes han llamado la atención sobre la importancia de la infraestructura de ciberseguridad. De 2020 a 2023, el número de Estados de América Latina con una estrategia nacional de ciberseguridad aumentó de 12 a 20. A este respecto, permítanme subrayar tres puntos.

En primer lugar, las actividades criminales en el ciberespacio crean y agravan amenazas para la paz y la seguridad internacionales, en tiempo de paz y conflictos armados. El derecho internacional humanitario prohíbe los ataques indiscriminados dirigidos contra los objetos civiles. Consideramos que, al aplicar este principio fundamental a las operaciones cibernéticas, los datos civiles deben gozar de la misma protección que todos los demás objetos civiles.

En segundo lugar, es fundamental tener una interpretación suficientemente amplia del concepto de daño. El derecho internacional humanitario no puede

limitarse a reglamentar sólo los casos en que las operaciones cibernéticas resultan en daños físicos. Seríamos ciegos ante las realidades del uso malicioso de las herramientas cibernéticas si el derecho no brindara protecciones también contra las operaciones que hacen inútil la infraestructura cibernética o inhiben su funcionalidad.

En tercer lugar, si bien todos debemos reforzar nuestra ciberseguridad, nuestro medio de protección más eficaz es un marco jurídico inequívoco y riguroso. De manera colectiva, debemos eliminar cualquier zona gris que pueda permitir o excusar actividades cibernéticas maliciosas. Ya sea mediante la adopción de interpretaciones suficientemente defensoras del marco jurídico existente o mediante el desarrollo de nuevas normas jurídicas universales, la necesidad es urgente y el momento es ahora. Mientras tanto, la agenda de Protección de Civiles (POC) debería también abarcar las actividades cibernéticas que afectan a la población civil.

Señor Presidente,
Los Estados más pequeños como el mío dependen de un sólido sistema de derecho internacional para mantener la paz y la seguridad internacionales. Debe ser sólido en el papel y, lo que es más importante, debe ser aplicado con rigor y responsabilidad por todos los actores.

Muchas gracias.

Mr. President,
I thank the Republic of Korea for organizing this Arria-formula meeting.

Malicious activities in cyberspace carry grave consequences. I speak not in the abstract, but from concrete experience. Costa Rica was the victim of two significant ransomware attacks in 2022, which targeted 27 of our government bodies and then our healthcare system. This led to unprecedented disruptions to our economy, health care, and other crucial government sectors such as our social security system.

We declared a state of emergency and requested assistance from governments and nongovernmental leaders in the digital arena. The groups conducting these attacks announced themselves publicly, and their home State of operations is believed to be known.

Recovery did not take place all at once. It was a long, costly, painful process because of the encryption of the data of our government and citizens. We know that

we are not alone in our experience, but some choose to quietly acquiesce to the demands of the hackers instead of speaking out about their experience. These incidents drew attention to the importance of cybersecurity infrastructure. From 2020 to 2023, the number of Latin American States with a national cybersecurity strategy grew from 12 to 20. In this regard, please allow me to stress three points.

Firstly, criminal activities in cyberspace create and exacerbate threats to international peace and security, in peacetime and armed conflict. International humanitarian law prohibits indiscriminate attacks directed at civilian objects. We consider that when applying this fundamental principle to cyber operations, civilian data must enjoy the same protections as all other civilian objects.

Secondly, it is crucial to have a sufficiently broad interpretation of the concept of damage. International humanitarian law cannot limit itself to only regulating instances where cyber operations result in physical damage. We would be blind to the realities of the malicious use of cyber tools if the law did not also protect against operations that render cyber infrastructure useless or inhibit its functionality.

Thirdly, while we must each bolster our cybersecurity, our most effective means of protection is an unambiguous and rigorous legal framework. Collectively, we must remove any grey area in the law that might permit or excuse malicious cyber activities. Whether we do so by adopting sufficiently protective interpretations of existing law or by developing new universal legal standards, the need is urgent and the time is now. In the meantime, the Protection of Civilians Agenda (PoC) should also encompass cyber activities that impact civilians.

Mr. President,
Smaller States like my own rely on a robust system of international law to maintain international peace and security. It must be strong on paper, and more importantly, it must be thoroughly and responsibly implemented by all actors.

I thank you.

Bangladesh

Mr. Chair,

Allow me to thank Permanent Missions of the Republic of Korea, along with the United States and Japan, for convening this important meeting. I also thank the briefers for their valuable briefing.

In the evolving digital landscape, cyber threats loom large and very often imminent, disrupting global financial, democratic, socio-cultural and security structures. The 2024 Global Risks Report underscores cyber threats as one of the gravest challenges of our time, estimating potential cybercrime costs of $24 trillion by 2027. Such an astounding figure demand our immediate and urgent action.

Chair,

To answer your guiding questions, allow me to highlight the following points:

First, the proliferation of cyber threats, including ransomware attacks, cyber espionage, and mis and disinformation campaigns through deep fakes, poses significant risks to global peace and stability. These threats not only target critical infrastructure but also undermine democratic processes and societal harmony, including through spreading xenophobia, intolerance and stereotyping.

Additionally, advancements in artificial intelligence and quantum computing have magnified the scope and complexity of cyber-attacks. With billions relying on digital platforms for daily activities, the urgency to address these threats has reached unprecedented levels.

Second, we firmly believe that in the face of such a grave threat, we are only as strong as our weakest link. Therefore, enhanced international cooperation and coordination are indispensable today. Strengthening cybersecurity measures, fostering information sharing mechanisms, and investing in capacity-building initiatives are imperative to bolster resilience against cyber threats. In this regard, we emphasize the importance of upholding the principles of sovereign equality and international law in the digital domain. We must sort out ways and means to strike balance between freedom of expression and harmful dissemination of misinformation.

Third, in this rapidly evolving cyber landscape, we commend the Open-Ended Working Group on ICT security for facilitating vital international discourse and collaboration. The General Assembly, reflecting global will and aspirations of the international community, remains the key platform for such critical discussions, enabling all States to actively participate in shaping our collective cyber future. We also hope that Global Digital Compact will also be an important opportunity to address this issue, and the General Assembly and the Security Council would undertake a collaborative approach in its effective implementation.

Finally, we must work together to develop norms, standards, and regulations that promote a safe, secure, non-discriminatory and stable digital environment for all. The Council could play a vital role in fostering confidence building measures, including through effective information sharing, in this regard. Bangladesh reaffirms its commitment to collaborating, bilaterally and multilaterally, with the global community to address the evolving global cyber security threat landscape.

I thank you.

Liechtenstein

Mr. President,

We thank the Republic of Korea, Japan and the United States for continuing the recent trend of engaging the Security Council on the topic of cybersecurity, with Estonia convening the first Security Council open debate on cyber security during its Presidency in June 2021. Security Council engagement with this topic helps ensure that the rule of law effectively addresses modern technological challenges, including the proliferation of cyber threats, which is crucial for its mandate to maintain international peace and security.

The escalating sophistication and frequency of cyberattacks, as exemplified inter alia through the aggression against Ukraine, underscore the imperative for clarity regarding the application of international law to malicious cyber activities. It is clear that cyberwarfare is subject to international law – including international humanitarian law and international criminal law, inter alia under the UN Charter, the Geneva Conventions and the Rome Statute of the International Criminal Court. The International Committee of the Red Cross (ICRC) has affirmed that international humanitarian law extends to cyber operations during armed conflicts, emphasizing the need for adherence to legal standards even in the digital realm.

As discussions on the application of international law to cyberspace continue in various international fora, including the United Nations, it is imperative to integrate the Rome Statute and international criminal law into these deliberations. Liechtenstein, in collaboration with ten other ICC State Parties, has convened a Council of Advisers on the application of the Rome Statute to cyberwarfare, which produced a report on how each of the Rome Statute's four core crimes, the crime of aggression, war crimes, crimes against humanity and genocide, apply in the context of cyber operations. Prosecuting cyber and cyber-enabled crimes at the ICC is instrumental in addressing the evolving cyber threat landscape effectively, including through Security Council referrals to the Court, in order to collectively ensure that justice is not outpaced by the shifting nature and tools of war.

The ICC Prosecutor has also recently discussed the potential for the ICC to prosecute 'cyberattacks' as international crimes pursuant to the Rome Statute. We welcome the new multi-stakeholder consultation process that he has initiated with Microsoft to

develop an official policy to address cyber-enabled crimes through the Rome Statute system. As cyber capabilities evolve and proliferate among both State and non-State actors, there is an urgent need for concerted efforts to address cyber threats comprehensively.

I thank you.

The Republic of Philippines

Co-chairs, Honorable members of the Security Council,

The Philippines extends its gratitude to the Republic of Korea, Japan, and the United States of America for convening this crucial Arria Formula Meeting, focusing on the evolving cyberspace landscape and its implications for international peace and security. As we gather today, it is imperative to address the pressing challenges posed by malicious cyber activities, which continue to threaten the stability of nations worldwide.

Reflecting on the objective of this meeting, the Philippines underscores the need to raise awareness and promote better understanding of the multifaceted nature of cyber threats, including ransomware, crypto-heists, and financial crimes involving advanced cyber techniques. These malicious activities not only jeopardize the integrity of our digital infrastructure but also have far-reaching implications for both public and private sectors globally.

In response to the guiding questions before us, I wish to highlight the following:

First, the Philippines acknowledges the key emerging trends of malicious activities in cyberspace, which pose additional challenges to international peace and security. Recent cybersecurity breaches in our country, including the defacement of government websites, data breaches targeting critical institutions, and large-scale theft of personal information, underscore the severity of the threat we face.

Second, criminal activities in cyberspace serve as a significant threat multiplier, exacerbating existing challenges to international peace and security. The Philippines has experienced firsthand how cyberattacks can disrupt essential services, undermine trust in institutions, and have profound socio-economic impacts, further complicating efforts to maintain stability.

Third, the increasing accessibility of advanced cyber tools and techniques to both state and non-state actors have profound implications for international peace and security. The democratization of cyber capabilities has lowered the barriers to entry, empowering malicious actors to launch sophisticated cyberattacks with impunity, transcending geographical boundaries.

In response to these challenges, the Philippines emphasizes the importance of collective measures and innovative strategies to counter cyber threats effectively. Collaboration among states, international organizations, and relevant stakeholders is paramount to enhance cybersecurity resilience, mitigate risks, and strengthen deterrence mechanisms.

In this regard, we are pleased to share that on the occasion of the recent state visit of President Ferdinand R. Marcos, Jr. in Australia last month, Government of the Republic of the Philippines and the Government of Australia signed a Memorandum of Understanding on Cyber and Critical Technology Cooperation. This is a significant step towards bolstering our cyber capabilities and fostering regional collaboration. For the Philippines and the developing South, we need more partnerships like this in support of narrowing the digital divide and transferring technologies.

Furthermore, the Philippines recognizes the pivotal role of the UN Security Council in addressing the evolving nature of cyber threats within its mandate of maintaining international peace and security. While we give primacy to the ongoing discussions in the Open-Ended Working Group on the Use and Security of ICT, we must also ensure that the Security Council remains actively engaged in shaping the global cybersecurity agenda.

Finally, Co-chairs, the Philippines reiterates its commitment to enhancing cyber resilience and promoting responsible behavior in cyberspace. We call for continued cooperation, capacity-building efforts, and the establishment of mechanisms, including a regular trust fund, to support developing countries in addressing cyber threats effectively. As we navigate the complexities of the digital age, let us work together to safeguard the integrity of cyberspace and uphold the principles of peace and security for all.

We also thank our briefers from UNODA, UNIDIR, and Chainalysis.

Thank you, Co-Chairs.

Pakistan

Chair,

We thank the Republic of Korea, Japan, and the United States for organizing today's meeting. We also thank the briefers for their useful insights**.**

Pakistan acknowledges the gravity of the evolving cyber threat landscape and its implications for international peace and security. We also recognize the urgency in addressing key emerging trends of malicious activities in cyberspace, including ransomware, and the theft of sensitive information through techniques like phishing,

We are particularly concerned at the significant increase in recent years in the frequency of cyber attacks on critical infrastructure.

Another aspect of cyber threat which several countries, including my own are suffering is the disinformation. This facet of global cyber warfare not only constitutes interference in the internal affairs of states, but also erodes international cooperation and potentially threatens international peace and security.

This in view, it is essential to build defence against the evolving cyber threat landscape. In this regard, my delegation wants to make the following three points:

- **First,** it is essential to bridge the growing digital divide between the developed and developing states, which is highest priority for developing countries;

- **Second:** capacity building has a crucial role to play in effectively responding to current and potential cyber threats. The need for capacity building becomes more important because of the large gap in terms of capacities and skills between States;

- **Third,** International cooperation, especially in real-time information sharing is paramount for comprehending and combating evolving cyber threats.

Chair,

The UN Charter is unequivocal in upholding the principles of sovereignty, territorial integrity and non-interference in the internal affairs of States. These principles should serve as a guiding framework as we navigate the complexities of cyber governance.

A simple assertion, however, of the applicability of existing international law to cyber space is not sufficient to address the multifaceted legal challenges arising from ICTs. Pakistan therefore shares the view that it is essential to develop a legally binding international instrument, specifically tailored to the unique attributes of ICTs. Such a legal framework should continue to be discussed in the ongoing OEWG on ICTs. This OEWG is also well placed to discuss and finalize the ToRs and the mandate of the future platform to be established after the conclusion of the OEWG in 2025.

I thank you.

Latvia

Co-chairs,

Latvia welcomes this Arria meeting organized by the Republic of Korea together with the US and Japan. We thank all the briefers for their insightful presentations.

Co-chairs,

Security considerations have always been integral part of the development of cyberspace. The first computer virus as well as antivirus codes were developed already in the early seventies of the 20th century, well before formation of the internet as we know it. The cyber-attacks we all face today are becoming more sophisticated, destructive and frequent than ever.

However, as stated by the UN High Representative for Disarmament Ms Nakamitsu, “cyberspace is not a lawless space”. It has been concluded in several reports of the UN Group of Governmental Experts, as well as Open Ended Working Group that international law, including international humanitarian law, is applicable to cyberspace.

Therefore, the question is not about the rules governing cyberspace, but rather about ensuring their implementation. In this regard, ransomware, indeed, serves as a suitable example of a growing cyber threat that demands coordinated response by the international community.

Ransomware attacks have affected many states and regions, including Latvia. My country’s response has been focused on building national cyber resilience. It includes steps aimed at strengthening cyber defence through coordinated actions by relevant institutions such as CERT, State Police and Ministry of Defence. They are proactively implementing defensive measures, including cyber threat hunting operations, as well as phishing and malware tests for the operators of critical infrastructure. We pay equal attention to strengthening cyber literacy and hygiene in the public sector and society as a whole. Ability to recognize and prevent malware from activating is much more effective than attempting to contain it.

Building on our national steps, we are sharing our experience with partners and participating in international coordination efforts. While supporting current negotiations in the OEWG, Latvia believes that cybersecurity matters deserve a permanent UN mechanism. The proposal to establish the UN Programme of Action (PoA) on cybersecurity has received a wide cross-regional support and we are awaiting its establishment no later than in 2026.

That said, we do not regard cybersecurity as a matter belonging only to the GA. The Security Council should continue to deliberate on cybersecurity matters, including to reinforce application of international law in cyberspace. As we proceed towards establishment of the PoA, it would be worth exploring options for interaction between this mechanism and the Security Council. It would help ensure that the Council is kept abreast with the developments in the cyber domain and is in position to take the necessary decisions.

I thank you.

Morocco

Mr Chair,

1. Allow me at the outset to thank you for convening this timely and very important Arria formula meeting on Cybersecurity threats and their implications for the international peace and security.

2. I express also my delegation's deep gratitude to the esteemed briefers for their participation and insightful remarks.

Mr Chair,

3. The **ICTs** have catalyzed transformative growth worldwide, enhancing efficiency, productivity, and work-life balance. These technologies have significantly advanced human progress and fostered global cooperation. However, they also **pose tremendous cybersecurity risks that impact individuals, entities, and Member States in different ways.**

4. Cyber threats have become a significant concern in the international security landscape and were discussed several times in the UN Security Council. In this regard, **my delegation estimates that the following elements may be considered as a part of the global reflection upon the growing importance of cybersecurity in maintaining international peace and security**, namely by:

- Reaffirming that cyber threats can jeopardize international peace and security by targeting critical infrastructure, disrupting essential services, and potentially leading to conflicts.
- Continue to tighten the noose on terrorist groups and criminal organizations as they are increasingly leveraging the cyber domain for malicious activities, including data theft, financial fraud, and potential attacks on critical infrastructure.
- Promote the ongoing efforts within the UN is terms of establishing norms of responsible behavior in cyberspace, including discussions on the applicability of existing international law, such as the UN Charter, to cyber operations.

5. As we are halfway through the Open-Ended Working Group (OEWG) on Information and Communication Technologies, and we have come a long way since this OEWG started in 2021, allow me to express my delegation's deep gratitude to the Chair of this Group, H.E.Mr Burhan Gafoor and his team for their tireless efforts aiming to realize concrete steps forward across all aspects of the OEWG mandate, and preserve a very high level of participation and substantive engagement within this important process.

Mr Chair,

6. Promoting confidence-building measures within the framework of cybersecurity issues, could highly lead to effective communication between Member States and bridging perspectives, with the aim of avoiding escalation and preventing conflicts between Nations in the cyberspace.

7. In the same vein, my delegation sees the merit of examining ways to benefit at the international level from confidence-building measures formulated at the regional and sub-regional levels, within the framework of the United Nations, regarding the suitability and benefit of these measures.

8. Bearing in mind the rapid growth of the use of ICTs and the increasing reliance on digital systems, we would like to **emphasize the importance of international cooperation and assistance to support developing countries in building their relevant national capabilities. Thus, enabling digital access for all without discrimination, and providing the resources needed by these countries to address the increasing threats in cyberspace.**

9. To conclude Mr. Chair, Morocco has been continuously a fervent promoter to the UN central role in increasing international and regional coordination within Member States concerning cybersecurity issues, in order to avoid duplication of efforts and maximize the available resources. In this regard, I can ensure you that Morocco will maintain its constructive engagement and full support to **collective efforts to ensure an open, secure, stable, accessible and peaceful ICT's environment**. **Only by working together, we can create a better world that keeps humanity safe from existential threats and technological harm in times of war.**

I thank you for your kind attention.

Qatar

Excellencies, distinguished delegates, ladies and gentlemen,

- I would express our gratitude to the Republic of Korea for convening this crucial meeting, and our appreciation extends to the UNODA, UNIDIR, and the private sector representatives for their valuable insights.

- The State of Qatar emphasizes the importance of addressing these evolving cyber threats through international cooperation and collaboration. We believe that a collective approach is essential to effectively combatting cyber threats and mitigating their potential impact on international peace and security.

- We also would like to highlights the dire importance of sharing best practices and local experiences from the global stage in all landscape of information and communications technology (ICT) security. This is integral to fostering confidence in this critical and strategic field, while recognizing the imperative of confronting risks and threats in a collective manner.

- The State of Qatar recognizes the escalating complexity and sophistication of cyber threats, which pose a direct threat to the stability of nations and the global community as a whole.

- We support the call for increased dialogue and information-sharing among nations, as well as the development and implementation of robust cybersecurity measures at both national and international levels. We stress the importance of adhering to established norms and principles of responsible state behavior in cyberspace, as endorsed by the United Nations General Assembly.

- Encouraging collaborative accomplishments, we emphasize the importance of strengthening partnerships between the public and private sectors. It is imperative to incorporate this aspect into the officially endorsed list of confidence-building measures. Our standpoint is influenced by the State of Qatar's effective initiatives in enhancing such partnerships within the national level, resulting in tangible outcomes. Particularly in the realm of safeguarding the digital environment, accreditation certificates have been instrumental in cultivating trust and credibility between consumers and service providers.

Consequently, this has motivated service providers to improve their cybersecurity protocols and enhance the skills of their employees.

- We firmly believe that these initiatives, plans, and frameworks will catalyze joint actions between the public and private sectors in formulating regulations, policies, and strategies aligned with international standards and best practices. Such alignment will not only bolster confidence in the digital environment but also boost the cybersecurity sector towards fostering innovation and sustainable development.

- The State of Qatar unveiled guidelines for the application and safe utilization of artificial intelligence during the Safe Use of Artificial Intelligence conference in Doha on February 20, 2024.
    - This initiative aligns with global endeavors aimed at establishing regulations for governing artificial intelligence to mitigate security vulnerabilities within this realm.

- In conclusion, the State of Qatar reaffirms its commitment to actively engage in international efforts to strengthen cybersecurity and counter cyber threats. Through collaboration and cooperation, we can effectively safeguard international peace and security in an increasingly digitized world.

Israel

Thank you Chair for giving us the floor during this very important and timely Arria Formula discussion.

Cyber threats today are affecting all nations, and do not distinguish between entities or people, and that is why we need to work together and unite against those threats.

Israel is considered one of the most attacked nations in cyber and our critical infrastructure, essential services, the government, public and private sectors are targets of numerous malicious efforts to penetrate and damage our digital domain. It is the continuity of these basic and essential services to the public that are at stake here.

Since the October 7th heinous terror attack against Israeli citizens, around 15 cyber attack groups attributed to malign states and other terrorist and non-state actors have intensified their attempts to launch cyber-attacks against targets in the Israeli public, private and government sectors. The attacker's intention, as any other terror organization, is to spread terror by harming civilians and attempting to cause real damage. They have been using cyberspace to damage, among other things, our critical civilian infrastructures, targeting our energy installations, water systems and even hospitals. Their actions should be condemned uniformly, also in this forum.

Mr. Chair,

An additional threat is the one posed by malicious actors using cyber sphere to conduct influence operations through spreading misinformation and fake-news and engaging in sophisticated phishing campaigns aiming to spread their malware. This is particularly serious as it can directly threaten democratic processes and harm nations national security. We should all work together to improve our capabilities to fight these and similar threats.

We would like to highlight the emerging threat emanating from collaboration between rogue states and malicious non-state actors such as: organized criminal actors and terrorist organizations acting as proxies. The proliferation and availability of advanced cyber tools in the hands of malicious non-state actors and unauthorized private actors constitutes a serious threat. The malicious use of these sophisticated intrusive cyber capabilities by malicious non-state actors and unauthorized private entities carries serious implications to national security. In many cases these malicious actors also

receive support and safe havens through states, which enables them to pursue their harmful activities with impunity.

One of the most notorious uses of cryptocurrency in cybercrime is ransomware. One of today's most persistent cyber security problems, especially for organizations. Ransomware attacks have also increased in parallel with the rise of cryptocurrencies. In this context the illicit financing of cyber-attacks using crypto currency is a growing threat. This is an area where countries could collaborate to block the funding for malicious cyber activities. We believe that if we could develop an efficient mechanism to freeze and seize crypto currencies on a global scale, we could drastically prevent many of these cyber-attacks.

One of the practical solutions offered to enhance cooperation and info sharing between states and stakeholders is the "Crystal Ball" platform - an advanced cloud platform encompassing countries and partnerships, the result of a collaboration between Microsoft, the Israeli National Cyber directorate, and the United Arab Emirates Cyber counsel. Its purpose is to enable the analysis and sharing of information in an interactive, fast, safe, and easy way between countries on cyber defense issues. platform is designed as part of the International Counter Ransomware Initiative, a global initiative led by the White House that aims to deal with the ransomware threat worldwide.

To conclude Mr. Chair, Israel is looking to cooperate with other states on the prevention and mitigation of existing and emerging risks and threats in the cyberspace, aiming at building together a stronger global resilience.

Thank you Chair.

Uruguay

Señor Presidente,

Deseamos agradecer la invitación de la República de Corea para participar de la Formula Arria sobre Ciberseguridad. Esperamos que este encuentro nos permita generar mayor entendimiento sobre la complejidad que revisten los temas vinculados al uso malicioso de las TICs y promover un abordaje multifactorial sobre la naturaleza de los conflictos internacionales.

Los desafíos en materia de la ciberseguridad son urgentes y requieren de una acción mancomunada de la comunidad internacional para hacerles frente de manera eficiente y sostenible. Uruguay expresa su preocupación por el crecimiento exponencial de los ciberataques en sus distintas formas y objetivos, como el *ransomware, malware, phishing, etc.* Puntualmente, se destacan por sus efectos destructivos y desestabilizadores, aquellos ataques destinados a las infraestructuras críticas de los Estados, como pueden ser los hospitales, plantas potabilizadoras de agua, etc.

De la misma manera, observamos con atención el avance de la inteligencia artificial con los desafíos y beneficios que esta conlleva.

En este contexto desafiante, Uruguay se encuentra fortaleciendo su CERT, multiplicando su capacidad de monitoreo y minimizando los tiempos de detección y respuesta a los incidentes, generando una reducción del riesgo y ahorros significativos para el Estado. También estamos trabajando en automatizar las respuestas a los incidentes y utilizar inteligencia artificial para la detección de patrones, además de incorporar analítica de datos para realizar proyecciones y anticipar sucesos.

Uruguay promueve un enfoque de la IA que potencie las capacidades del ser humano, apuntando a mejorar la calidad de vida de las personas y agregando valor a las actividades humanas. Las soluciones que brinda esta herramienta deben atender el interés general, garantizando la inclusión y la equidad. Apoyamos que la IA sea utilizada de manera transparente, conociendo los algoritmos y datos utilizados, así como las pruebas y validaciones realizadas.

Señor Presidente,

Ante estos desafíos, los Estados debemos reaccionar con una mirada que promueva, proteja y asegure en primer lugar los derechos humanos en el ámbito cibernético, así como el derecho a la privacidad en la era digital. También debemos actuar motivados por el principio de buena fe en las relaciones internacionales y por el respeto a la Carta de las Naciones Unidas. Por esa razón, Uruguay hace un llamado a todos los miembros a avanzar en la aprobación de una Convención Internacional sobre Ciberdelito y continuar con las discusiones en el Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y las Comunicaciones y su Uso (2021-2025) con miras a generar un mecanismo permanente de acción.

Como lo reafirmábamos al comienzo de esta intervención, los desafíos que nos plantea el uso malicioso de las TICs deben ser enfrentados conjuntamente por la comunidad internacional. En ese sentido, la cooperación internacional resulta fundamental para un resultado exitoso y sostenible. Para ello, la creación de capacidades y transferencia de tecnologías en el ámbito de las TIC debe continuar siendo un pilar fundamental y transversal de todos los debates que se mantengan en las Naciones Unidas con miras a cerrar la brecha digital y de género.

Muchas gracias Señor Presidente.

Poland

Mr. Chair, Distinguished Delegates,

Poland fully aligns itself with the statement delivered by the European Union. Additionally, I would like to highlight a few elements in my national capacity.

The ongoing and rapid digitalization of all aspects of life and the functioning of states, economies and societies brings both tremendous opportunities as well as threats which are growing rapidly in number and complexity. Hence, the security of cyberspace is becoming the backbone of further development of states and harmonious relations among them. To this end, we need a closer cooperation based on trust within the UN framework. Poland believes that international law applies to cyberspace and must be observed. We are also of the view that the 11 voluntary norms of responsible state behaviour adopted by the UN in 2015 should serve as a foundation for our activities in cyberspace on the international level.

Regrettably, it happens quite often that international law and the voluntary norms are not observed. Some countries, which are very vocal about a need to adopt a new legally-binding instrument regulating the behavior of states in cyberspace, violate – on a daily basis - existing international law as well as the adopted norms. State actors conduct cyberattacks targeting, among others, critical infrastructure, public communication networks, health sector, government institutions, logistical systems as well as electoral processes.

Moreover, some states instead of fighting cybercriminals operating from their territories, groom and protect them for political or economic gain and in doing so, undermine the stability and security of others. The blurring of lines between state-sponsored and criminally motivated actors result in ambiguity when the victims of the attacks attempt to defend themselves and hold the perpetrators accountable for their malicious activities.

But there is also a large group of states which have an honest political will to implement international law and the voluntary norms but are lacking the necessary capabilities to do so. It is in our common interest to work closely together in order to assist them and offer them adequately measured and addressed capacity building. This will not happen overnight, therefore, we need a permanent platform for such cooperation within the UN

framework. In this context, Poland strongly supports the establishment of the Programme of Action. This initiative is aimed at the creation of a permanent, inclusive, transparent, results- and action-oriented mechanism of cooperation in the field of cybersecurity at the UN level. We encourage all UN members to support it and to actively contribute to its operationalization.

Thank you for your attention.

Bahrain

شكراً السيد الرئيس،

1. بداية يطيب لي أن أتقدم بالشكر إلى الوفد الدائم لجمهورية كوريا على عقد هذه الجلسة الهامة بمشاركة من وفدي اليابان والولايات المتحدة، كما أود أن أتقدم بالشكر إلى مقدمي الإحاطة على ما تفضلوا به من بيانات قيّمة.

السيد الرئيس،

2. إن المخاطر المتصاعدة التي تشكلها الأنشطة الخبيثة في الفضاء السيبراني مثل هجمات برامج الفدية، وسرقة العملات المشفرة، وسرقة المعلومات والأصول الحساسة لا تؤدي فقط إلى تعريض سلامة البنية التحتية الحيوية للخطر، بل تؤدي أيضًا إلى تفاقم التحديات القائمة التي تواجه الاستقرار العالمي، حيث تعمل هذه الأنشطة كمضاعفات قوية للتهديدات، مما يؤدي إلى تضخيم المخاوف الأمنية التقليدية وإنشاء نقاط ضعف جديدة، علاوة على أن الطبيعة المترابطة للأنظمة الرقمية تعني أن الحوادث السيبرانية يمكن أن تتصاعد بسرعة إلى أزمات دولية، مما يقوض الثقة والاستقرار بين الدول.

3. ومن هذا المنطلق، تشير مملكة البحرين إلى أهمية اتباع نهج متعدد الأوجه يتضمن الاستفادة من الأدوات والمنصات والأطر والاستراتيجيات الحالية والمبتكرة للتخفيف من المخاطر المرتبطة ببرامج الفدية وسرقة العملات المشفرة والتهديدات السيبرانية الأخرى، إلى جانب إشراك جميع أصحاب المصلحة بالنظر إلى أن الأدوات والتقنيات السيبرانية لم تعد مجالاً حصرياً للحكومات. كما تؤكد مملكة البحرين أهمية بناء القدرات وتبادل التكنولوجيات والمعرفة والممارسات الفضلى لتعزيز قدرات الدول على منع الحوادث السيبرانية والاستجابة لها.

السيد الرئيس،

4. على الصعيد الوطني، تولي مملكة البحرين اهتماماً كبيراً بأمن الفضاء السيبراني، وتستند في ذلك على منظومة واضحة لحوكمة أمن الفضاء الإلكتروني معززة باستراتيجية وطنية شاملة، حيث تم تأسيس المركز الوطني للأمن السيبراني سعياً إلى توفير فضاء إلكتروني آمن في مملكة البحرين عن طريق وضع معايير الحوكمة الفعالة، وتوفير وسائل الدفاع والمراقبة والاستجابة للهجمات الإلكترونية، فضلاً عن نشر الوعي بين الأفراد والمؤسسات.

5. وتمتد الاستراتيجية الوطنية للأمن السيبراني لتعزيز الشراكات الإقليمية والدولية، حيث تم تحديد خمس ركائز أساسية في هذه الاستراتيجية، وتعد كل ركيزة مكوناً أساسياً وضرورياً لتحقيق رؤية مملكة البحرين في مجال الأمن السيبراني، وتشكل بمجملها إطار عمل شامل ومتماسك للمحافظة على فضاء سيبراني آمن وموثوق، متمثلة في: حماية سيبرانية قوية ومرنة، الحوكمة والمعايير الفعّالة للأمن

السيبراني، بناء مجتمع واعي بالأمن السيبراني، تعزيز الحماية من خلال الشراكات والتعاون، وتطوير الكوادر الوطنية.

السيد الرئيس،

6. وفي الختام، تتطلع مملكة البحرين إلى المزيد من الحوارات المثمرة حول الأمن السيبراني في إطار الأمم المتحدة ولا سيما مجلس الأمن نظرا للطبيعة المتسارعة للتهديدات الناشئة عن التطورات المتصلة بتكنولوجيا المعلومات والاتصالات.

وشكراً السيد الرئيس.

Thank you Mr. President,

1. At the outset, I would like to extend my sincere appreciation to the Permanent Mission of the Republic of Korea for holding this important session in cooperation with the Permanent Missions of Japan and the United States. I would also like to extend my appreciation to the briefers for their valuable statements.

Mr. President,

2. The escalating risks posed by malicious activities in cyberspace such as ransomware attacks, cryptocurrency theft, and theft of sensitive information and assets not only jeopardize the integrity of critical infrastructure, but also exacerbate existing challenges to global stability, as these activities operate as powerful threat multipliers, amplifying traditional security concerns and creating new vulnerabilities. Indeed, the interconnected nature of digital systems means that cyber incidents can quickly escalate into international crises, undermining trust and stability between states.

3. In light of the above, the Kingdom of Bahrain stresses the importance of adopting a multi-faceted approach that includes leveraging existing and innovative tools, platforms, frameworks and strategies to mitigate the risks associated with ransomware, cryptocurrency theft and other cyber threats. We additionally encourage the engagement of all stakeholders given that cyber tools and technologies are no longer the exclusive domain of governments. The Kingdom of Bahrain also stresses the importance of building capabilities

and exchanging technologies, knowledge, and best practices to enhance countries' capabilities to prevent and respond to cyber incidents.

Mr. President,

4. At the national level, the Kingdom of Bahrain places great importance on the security of cyberspace, which is based on a clear system for cybersecurity governance reinforced by a comprehensive national strategy. The National Center for Cybersecurity was established in an effort to provide a secure cyberspace in the Kingdom by setting effective governance standards, providing means of defence, monitoring and responding to electronic attacks, as well as spreading awareness among individuals and institutions.

5. As for the National Cybersecurity Strategy, it is based on five basic pillars, each of which is an essential and necessary component to achieving the Kingdom of Bahrain's vision in the field of cybersecurity, and as a whole constitutes a comprehensive and cohesive framework for maintaining a safe and reliable cyberspace. These pillars are: 1) Strong and flexible cyber protection; 2) effective cyber security governance and standards 3) building a cyber security aware society; 4) enhancing protection through partnerships and cooperation; and 5) developing national cadres.

6. In conclusion, the Kingdom of Bahrain looks forward to continued fruitful dialogues on cybersecurity within the framework of the United Nations, especially the Security Council, given the accelerating nature of threats arising from developments related to information and communications technology.

I thank you.

Germany

Thank you, President.

Germany aligns itself with the statement of the European Union.

I would like to add the following remarks in national capacity.

Like other delegations, we want to thank the Republic of Korea for this initiative to discuss the evolving cyberthreat landscape and its importance for the maintenance of international peace and security.

We see merit in further exploring the role of the Security Council in this important field.

President,

we (all) face an increasingly complex landscape of cyberthreats.
Just last year, my own country, Germany recorded a record-high number of sophisticated ransomware attacks against critical infrastructure like hospitals. These attacks endanger public safety, patients' lives and public trust. Economic damages are in the billions.

"Ransomware-as-a-service" enables actors without technical skills to carry out ransomware attacks. The increasing proliferation of these malicious cyber tools contributes to blurring the lines between cybercriminals and state-controlled hackers acting upon political motives. It allows those actors the financing of illicit arms programs, which pose increasing risks to international peace and security.

We are convinced that we need to join forces to fight cybercrime.

Germany actively participates in the Counter Ransomware Initiative. In this initiative we strive to foster cyber resilience through greater international cooperation in the areas of capacity building and diplomacy.

President,

Germany is especially concerned about the use of cyber means in armed conflict.

We already observe worrying spillover-effects in our networks from the cyber dimension of international conflict. Both, state and non-state actors, are exploiting cyber vulnerabilities to advance their agendas. These patterns disrupt trust among nations and cause concern for the maintenance of international peace and security.

We therefore call on all states to adhere to the UN Norms of Responsible State Behavior in cyber space.

It is our firm conviction that the UN charter does apply in cyberspace.

As mentioned by the European Union, existing rules and principles of International Humanitarian Law place important limits on cyber operations.

We ask all states to work together in this spirit, in order to contribute to a safe and rules-based cyber space.

Thank you.

Italy

Mr. Chair,

I would like to thank the delegation of the Republic of Korea for organizing this Arria-formula meeting on cyber security, which provides an opportunity to increase our engagement on ensuring comprehensive security in the cyberspace, in light of increasing threats deriving from new technologies.

The evolving threat landscape in the cyberspace presents unprecedented challenges that demand collective action and innovative solutions. From a proliferation of malware to the theft of cryptocurrency, from ransomware attacks to the use of Artificial Intelligence to destabilize democratic processes and the development of autonomous weapon systems in warfare, the nature of cyber threats is constantly being redefined.

The threat posed by malicious cyber activities, particularly in the context of State-sponsored actors, cannot be overstated: we have the great responsibility for promoting a responsible behavior in cyberspace, thus preventing the latter's misuse by anyone. To achieve this goal, we need to continue working on a multistakeholder approach based on dialogue, transparency and confidence-building measures, improving and sharing awareness of cyber threats, and expanding our coordinated cyber response in line with our national security frameworks.

Additionally, cybersecurity of critical infrastructures is particularly important to guarantee access to life-saving information and services. These issues are more than ever pressing in the current challenging geopolitical environment, especially since Russia's unprovoked and unjustified war of aggression against Ukraine.

Italy is firmly committed to a global, open, free, stable and secure cyberspace, where international law, including international humanitarian law and human rights law, fully apply. With this regard, we welcome UNIDIR's activities aimed at raising awareness and sharing best practices among Member States about the interpretation and applicability of international law.

Moreover, we are strongly engaged in the promotion of the responsible and ethical use of AI, recognizing the necessity of a shared commitment to transparent and accountable practices in this domain. As emphasized by Prime Minister Meloni in her address to the General Assembly of the UN in September, we need global governance mechanisms that ensure that technologies respect ethical boundaries and that technological evolution is at the service of humanity and not vice versa.

The Italian Presidency of the G7 aims to translate the principles of safe, secure, and trustworthy AI into concrete and actionable policies. We welcome the recent adoption of the GA Resolution on AI for sustainable development, which Italy has co-sponsored, and we look forward to both the final report of the High Level Advisory Body on AI and the negotiations for the Global Digital Compact.

We also acknowledge capacity building as a crucial tool to share knowledge and experience for a safer and more secure cyberspace. Together, let us forge a path towards a future where new technologies serve as a force for good, bridging divides, propelling us towards the Sustainable Development Goals and enhancing global security.

I thank you Mr. Chair.

Czechia

Cybersecurity is playing a growing role in domestic and foreign policies of all nations and is gaining prominence on the agenda of international organisations. Cyberspace has become one of the major battlegrounds of geopolitical competition.

The threat landscape is rapidly evolving. We are witnessing a deterioration of the international environment. Malicious cyber activities are becoming more complex and dangerous as our reliance on ICT technologies grows.

Individual and national cyber resilience cannot be strengthened without strong international partnerships. That is why Czechia is holding a number of dialogues on cyber security with countries in Africa, the Indo-Pacific and Latin America.

Cybercrime in the Czech Republic has doubled in the past period. The number of cyber incidents within the critical information infrastructure also doubled, with the majority of them being attacks on the availability of services.

Ransomware attacks have long been among the most serious cyber threats. A rapidly growing trend is ransomware-as-a-service. That is why Czechia joined the International Counter Ransomware Initiative, including its 2023 Joint Statement, and actively supports multilateral efforts in this area.

Apart from cybercrime groups, state-sponsored cyber actors remain the biggest threat to Czech cyber security. Czechia remains strongly committed to the adherence to the UN framework of responsible state behaviour in cyberspace. The framework has been endorsed by all UN states, but clearly not all of them respect it. As stated in our recent National Position Paper on the Application of International Law in Cyberspace, Czechia fully endorses the international order based on international law that promotes an open, secure, stable, accessible and peaceful ICT environment. We consider international law to be a fundamental element of the framework for responsible State behaviour in cyberspace and reaffirm that international law, including the United Nations Charter in its entirety, is applicable to State conduct in Cyberspace. We applaud the African Union for achieving a common position on the topic, which shows that it is important for states to express their opinions in order to establish a global consensus.

Czechia is fully committed to advancing the global debate on countering cyber threats in the UN. We have actively participated in the Open-ended Working Group for

cybersecurity and Ad-hoc Committee on Countering the Use of Information and Communication Technologies for Criminal Purposes since their establishment.

We support an establishment of a permanent, single-track, inclusive and action-oriented mechanism under the auspices of the UN upon conclusion of the current OEWG in 2025, and we believe the Programme of Action on cybersecurity could be such a mechanism. Our long-term goal is to emphasize human-centric and human-rights based approach when addressing issues related to new technologies and cybersecurity. The human rights and freedoms must be protected both online and offline. Therefore, Czechia initiated and together with Maldives, Mexico, the Netherlands and South Africa presented a new UN resolution on promotion and protection of human rights in the context of digital technologies, which was adopted by consensus at the UN General Assembly last December.

In conclusion, I want to emphasize that in the context of the Russian illegal and brutal aggression against Ukraine, Czechia remains deeply concerned by Russian malicious cyber activities and disinformation that are targeting not only Ukraine but also countries that support Ukraine’s legitimate right to defend its sovereignty and territorial integrity.

Estonia

Mister/Madame Chair,

We welcome today's discussion and thank the briefers for their valuable insight. Estonia aligns with the Statement delivered by the European Union.

Mister/Madame Chair,

Since Estonia introduced the topic of cyber security to the Council three years ago, the security and stability of cyberspace has remained of great concern to us. We are reminded daily that open, secure, stable, accessible and peaceful ICT environment cannot be taken for granted and is not separate from the physical world.

We are increasingly alarmed by the sheer amount as well as the damage caused by cyber threats carried out by both State and non-State actors. We see how Russia's kinetic aggression against Ukraine is accompanied by malicious cyber operations and how this combined warfare paves the way for the future conflicts. In other cases, cyber operations have been so severe that they resulted in the declaration of a state of national emergency. Thus, there are clear implications on international peace and security, calling for the attention of the Security Council.

Importantly, we call for the strengthening of the international rules-based order. We need to hold accountable the actors responsible for malicious operations in cyberspace and adhere to international commitments.

Mister/Madame Chair,

States need to invest in cyber resilience long before malicious cyber operations take place. National strategies are a prime tool for identifying domestic roles and responsibilities, outlining national priorities and challenges, offering a comprehensive approach to awareness raising and education as well as mapping relevant international processes.

Equally, Estonia believes that security comes from information sharing and international cooperation. We invite States be open about threats and vulnerabilities, actors and their capabilities. Typically, the consequences of the vulnerabilities depend on the speed with which we act – whether we are aware and able to patch them before criminals manage to exploit them.

Mister/Madame Chair,

In conclusion, the Security Council should continue to exchange views on existing and potential cyber threats and thereby raise awareness of the strategic implications of these security challenges. Deepening these discussions and developing a comprehensive approach to enhancing cyber resilience will support States in taking appropriate technical, legal, policy and other measures to protect their systems.

Thank you.

Ukraine

Mr. Chair,

We are grateful to the Republic of Korea, Japan and the United States for convening this timely Arria-formula meeting on threats in cyberspace. We also extend our appreciation to all briefers for their remarks.

For the last decade, cyber threat landscape has become more complex and challenging as ever before.

We are witnessing the growing number of cyber-attacks impacting critical infrastructure and critical information infrastructure, including those objects that provide essential services across borders and jurisdictions.

Notwithstanding that the international community has agreed on the framework of responsible behavior in cyberspace, certain States do not comply with this framework.

As indicated in the report of the 1718 Committees' panel of experts, the DPRK has been engaged in cyber espionage and cryptocurrency theft for further illicit funding of its weapons of mass destruction and ballistic missiles programs.

We express our solidarity with Albania, Australia, Costa Rica, Montenegro, and the United Kingdom, who have earlier experienced the impact of major malicious cyber activities against their critical infrastructure or public services.

We are concerned by growing number of cyber operations against democratic and electoral processes.

Since the launch of Russian Federation's full-scale invasion of Ukraine, our State has been facing the Russian persistent cyber-attacks alongside with its conventional warfare. In fact, Moscow has been waging a first ever war in cyberspace.

In addition to governmental entities, the main targets of Russian cyber operations are critical information infrastructure and critical infrastructure, including banking structures.

They conduct information operations and attack telecommunication systems to deprive citizens of access to mobile communications and the Internet.

In order to effectively prevent, combat and mitigate cyber threats, Ukraine actively participates in the work of international platforms, including on capacity-

building, exchanges of information, and collaborates with international partners, particularly NATO and the EU.

We stress the importance of ensuring accountability for malicious cyber activities. In this respect, Ukraine has started to investigate and prosecute cyber-attacks as war crimes.

We encourage the UN Member States to continue working on implementing principles of responsible state behavior, raising awareness, building capacities, especially in the light of existing and emerging threats in cyber domain.

Thank you.

Chile

We would like to thank the Permanent Mission of the Republic of Korea for this Arria-Formula meeting about the evolving cyberthreat landscape and its implications for the maintenance of international peace and security.

Chile considers that cyberattacks and malicious activities in cyberspace are a threat to international peace and security and may affect States in different ways depending on their levels of digitalization, capacity, security and resilience of information and communications technologies, its infrastructure, and development. With special attention, we emphasize that these threats can also differentially affect various groups and entities, especially keeping in mind women, girls, boys, and teenagers.

For this reason, we believe that it is essential to strengthen the joint work and cooperation between States. That includes the exchange of experiences and lessons learned, the implementation of existing norms of responsible state behaviour in cyberspace, the application of international law and international humanitarian law, confidence building measures and capacity-building, all which help to reduce mistrust among states and contribute to stability in the cyber domain.

Now we will address some of the guiding questions:

Regarding the emerging and evolving trends of malicious activities in cyberspace, we can mention the use of AI and machine learning, the combination of diverse attack vector tactics, supply chain attacks that compromise the integrity of products and services, crypto-heists, IoT Device Attacks, among others. At the same time, the second annual progress report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, mentions that States also highlighted the risk posed by malicious software such as ransomware, as well as wiper malware and trojans, and techniques such as phishing and distributed denial-of-service (DDoS) attacks.

Regarding the second question, cyber criminal’s activities can deeply impact the global economy, national security, social stability, and individual interests. The cost of cybercrime could reach $10.5 trillion annually by 2025, according to the World Economic Forum. Since cyber criminal’s activities are increasingly targeting critical infrastructure and governments, they scale up tensions between states, damaging trust and affecting international security as well. The identification of malicious activities and such actors that undermine international security and stability through specific reports has been a valuable tool and in this regard, we deeply regret the veto against the extension of the

mandate of the Panel of Experts assisting the 1718 DPRK Sanctions Committee. We thank and recognize the valuable work that the Panel has done since its establishment.

To confront these threats mentioned before, States can establish collaboration frameworks for the exchange of information, technical entities meetings at the bilateral, multilateral, and especially regional levels, along with coordinated work and partnership with the private sector and other interested parties, using technical and diplomatic points of contact, and promoting meetings and tabletop exercises. The UN Global POC directory will be key in this matter.

It is also important to develop greater capabilities in the field of cyber intelligence, along with efficient mechanisms for the exchange of information, as well as the necessary and progressive adaptation of regulatory frameworks. Likewise, it is essential that States be able to have permanent training programs, particularly for government entities. Developing Structures and coordination plans is important, but not only at the government level, but also to strengthen effective partnerships with civil society, the private sector, technical community and academia.

In this regard, we believe the Security Council plays an important role to advance discussions on cyber threats to peace and security. It could also play a role in building consensus around confidence-building and cooperative measures, including prevention and risk reduction in the use of ICTs by states, and the protection of civilians and critical infrastructure in conflict situations, identifying measures to support capacity-building.

Mexico

México da la bienvenida a esta reunión bajo fórmula Arria que busca dar continuidad a las discusiones que han tenido lugar bajo el auspicio del Consejo de Seguridad, así como a los avances logrados en el marco del Grupo de Trabajo de Composición Abierta sobre Ciberseguridad de la Asamblea General.

Dada la naturaleza dinámica de las amenazas cibernéticas, México sigue apostando por el multilateralismo y la cooperación internacional para prevenir, mitigar y controlar los incidentes cibernéticos maliciosos que repercuten en la paz y en la seguridad.

En éste y otros foros, México desea subrayar que los problemas no provienen de las tecnologías como tal, sino de sus usos hostiles y delictivos. México privilegia una visión tecnológicamente neutra, centrada en la prevención y mitigación de incidentes, en la que la resolución de conflictos tenga lugar por medios pacíficos y diplomáticos.

México reitera su compromiso con la implementación del marco normativo derivado del Grupo de Expertos Gubernamentales (GGE) y el Grupo de Trabajo de Composición Abierta (OEWG 2021), así como de las recomendaciones contenidas en los dos informes de progreso anual (APR) derivados del Grupo de Trabajo 2021-2025. Estos últimos son para nosotros el sustento ideal para la aplicación práctica de las normas ya acordadas, así como de las medidas de fomento a la confianza (CBMs) para un ciberespacio seguro y respetuoso de derechos.

Como parte del compromiso en la aplicación de este marco, México hace un llamado a continuar profundizando sobre la aplicabilidad del derecho internacional, incluyendo el derecho internacional humanitario, en el ciberespacio. México continúa trabajando, de la mano de todos los actores relevantes, para identificar con mayor detalle las reglas y clarificar cómo se aplican específicamente a una gama de operaciones cibernéticas, como las que se han discutido en este espacio, así como discutir impactos particulares sujetos a la protección, tales como las infraestructuras críticas. El Consejo de Seguridad debe promover espacios de intercambio como éste para avanzar entendimientos comunes en torno a las amenazas y riesgos de las tecnologías digitales en su relación con el mantenimiento de la paz y la seguridad internacionales. A su vez, tiene la capacidad para respaldar y promover las normas para el comportamiento responsable en el ciberespacio mediante el cumplimiento del marco jurídico internacional. Consideramos que también resulta en un espacio efectivo para facilitar la ciberdiplomacia y el diálogo, y servir de plataforma para debatir,

compartir información sobre amenazas y promover respuestas colectivas. México apoya el intercambio continuo de información sobre ciberamenazas, así como el desarrollo y la mejora de plataformas para compartir dicha información, como el Directorio Global de Puntos de Contacto.

Resulta indispensable seguir trabajando para reforzar los marcos jurídicos para prevenir, combatir y judicializar eficazmente el ciberdelito. Con esto en mente esperamos que las negociaciones del Comité Ad Hoc para la elaboración de una Convención sobre el Ciberdelito, que se dan en el marco de la Tercera Comisión, puedan concluir con éxito este año. Finalmente, adoptar estas medidas colectivas y aprovechar el papel estratégico del Consejo de Seguridad representa para mi país una vía adicional para construir ciber resiliencia ante las actividades maliciosas, así como un compromiso compartido en tanto que nos adaptamos continuamente a tales amenazas.

Hacemos votos para que desde este espacio se facilite y promueva la integración de una perspectiva de género transversal que tenga en cuenta a los grupos de poblaciones en situaciones vulnerables. Igualmente consideramos de vital importancia las asociaciones público-privadas como eje rector.

Mexico welcomes this meeting under Arria formula that seeks to give continuity to the discussions that have taken place under the auspices of the Security Council, as well as the progress made within the framework of the Open-Ended Working Group. Given the dynamic nature of cyber threats, Mexico continues to support multilateralism and international cooperation to prevent, mitigate and address malicious cyber incidents that impact peace and security. In this and other forums, Mexico wishes to emphasize that threats do not derive from technologies as such, but from their hostile and criminal uses. Mexico privileges a technologically neutral vision, focused on the prevention and mitigation of incidents, in which conflict resolution takes place through peaceful and diplomatic means. Mexico reiterates its commitment to the implementation of the framework of norms derived from the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG 2021), as well as the recommendations contained in the two annual progress reports (APR) derived from the current OEWG. For us, the latter are the ideal support for the practical application of the already agreed standards, as well as the confidence-building measures (CBMs) for a safe and rights-respecting cyberspace.

As part of the commitment to the application of this framework, Mexico calls to continue delving into the applicability of international law, including international humanitarian law, in cyberspace. Mexico continues to work, hand in hand with all relevant actors, to identify in greater detail the rules and clarify how they apply specifically to a range of cyber operations, such as those that have been discussed in this space, as well as discuss particular impacts subject to protection, such as critical infrastructure. The Security Council must promote space for exchanges like this one to advance common understandings regarding the threats and risks of digital technologies and their relation to the maintenance of international peace and security. In turn, the Council has the capacity to support and promote standards for responsible behavior in cyberspace through compliance with the international legal framework.

We believe that it is also an effective space to facilitate cyber diplomacy and dialogue, and serve as a platform to debate, share information on threats and promote collective responses. Mexico supports the continuous exchange of information on cyber threats, as well as the development and improvement of platforms to share such information, such as the Global Directory of Points of Contact.

It is essential to continue working to strengthen legal frameworks to prevent, combat and effectively prosecute cybercrime. With this in mind, we hope that the negotiations of the Ad Hoc Committee for the elaboration of a Convention on Cybercrime, which take place within the framework of the Third Committee, can conclude successfully this year.

Finally, adopting these collective measures and leveraging the strategic role of the Security Council represents an additional avenue for my country to build cyber resilience to malicious activities, as well as a shared commitment as we continually adapt to such threats.

We hope that this space will facilitate and promote the integration of a cross-cutting gender perspective that takes into account groups in vulnerable situations. We also consider public-private partnerships as a guiding principle of vital importance.

Ghana

Mr. Chairman,

I would like to extend my gratitude to the Permanent Mission of the Republic of Korea, as well as the Permanent Missions of the United States and Japan, for convening this Arria Formula meeting on the evolving cyber threat landscape and its implications for international peace and security.

2. I would also like to express my appreciation to the briefers for the invaluable insights on the topic.

Mr. Chairman,

3. The evolving cyber threat landscape presents formidable obstacles to international peace and security.

4. Criminal activities in cyberspace serve as potent threat multipliers, exacerbating existing challenges to international peace and security on multiple fronts. These activities have the potential to disrupt essential services, undermine democratic institutions, and exacerbate geopolitical tensions. Moreover, the anonymity and global reach afforded by cyberspace enable malicious actors to operate with impunity, further complicating efforts to hold them accountable for their actions.

5. In our opinion, however, the root of the problem extends beyond the inherent vulnerabilities and flaws in technologies themselves. Human conduct plays a crucial role in exacerbating cybersecurity challenges. Both state and non-state actors utilize cyberspace and associated ICT tools for various nefarious purposes. The aggregate effect of these challenges goes beyond significant ethical and security challenges; it also poses ecological risks and undermines trust between States. These developments have profound implications for international peace and security, as trust is a cornerstone of diplomatic relations and cooperation among nations.

6. To address the escalating threats posed by cyber activities and enhance its capacity to respond effectively, the United Nations Security Council must take decisive action. Strengthening institutional mechanisms and improving coordination with other

relevant UN bodies and specialized agencies is essential to formulating a comprehensive and cohesive response strategy.

7. One crucial avenue through which the Security Council can bolster its response is by adopting a presidential statement that develops and promotes international norms, standards, and principles for responsible state behavior in cyberspace, drawing upon existing non-binding political norms established within the First Committee of the General Assembly and the forthcoming convention on cybercrime under the Third Committee of the UN GA. It is also imperative to ensure coherence and synergy between these efforts and other major instruments, such as the Budapest Convention.

8. It is also paramount that the Council prioritize robust capacity-building efforts aimed at enhancing the technological and institutional capabilities of all States, particularly those with limited resources. This includes training programs, workshops, and technical assistance initiatives to improve cybersecurity readiness, incident response capabilities, and regulatory compliance.

Mr. Chairman,

9. We wish to underscore the importance of adherence to established legal frameworks and norms governing State behavior in cyberspace. In this regard, we affirm that existing international law, including the Charter of the United Nations, applies to the use of Information and Communication Technologies (ICTs) by States.

10. Furthermore, we advocate for exploring further initiatives at the global level, including the development of comprehensive international guidelines for ICTs, promoting security, privacy, and accountability in their design and deployment. We also wish to bring to the Council's attention our support for a proposal made by Kenya in the First Committee's OEWG on the security of and in the use of ICTs to establish a UN threat repository, fostering global awareness and understanding of cyber threats. This repository would serve as a valuable resource for Member States, enabling them to access timely information and intelligence on emerging cyber threats, enhance their cybersecurity readiness, and facilitate coordinated response efforts. By promoting collaboration and information sharing among Member States, the establishment of a UN threat repository would strengthen collective efforts to address cyber threats and uphold international peace and security in the digital age.

11. By remaining proactive and adaptive in its approach to cybersecurity, the Security Council can play a crucial role in addressing this increasing important aspect of global security and contribute to the maintenance of international peace and security in the digital age.

Thank you.

Argentina

En primer lugar, la Argentina quisiera expresar su agradecimiento a la Misión Permanente de la República de Corea ante las Naciones Unidas, así como también a los coorganizadores (Estados Unidos y Japón) por organizar el diálogo sobre "El desarrollo de amenazas de actividades maliciosas en el ciberespacio y sus implicancias para el mantenimiento de la paz y la seguridad internacionales" subrayando su pertinencia así como la creciente implicación del Consejo de Seguridad en cuestiones relativas a la ciberseguridad.

Al respecto, la Argentina quisiera hacer hincapié en la importancia de que las discusiones en el seno del Consejo de Seguridad en materia de ciberseguridad se nutran y generen mecanismos de sinergia con los debates que tienen lugar en el Grupo de Composición Abierta sobre Seguridad y en el uso de las Tecnologías de la Información y Comunicación.

Por otro lado, mi Delegación es consciente de la creciente evolución y complejidad de las amenazas cibernéticas, incluyendo los ataques con ramsomware y los cripto-atracos, los cuales representan no sólo un desafío para el mantenimiento de la paz y la seguridad internacionales, sino también para nuestra seguridad económica y social. Ello, se experimentó a través de ataques contra infraestructura crítica en varios países del mundo, incluyendo de nuestra región.

-Las Tecnologías de la Información y Comunicaciones poseen una naturaleza evolutiva que brinda enormes oportunidades de desarrollo económico y social a nivel global, pese a los enormes esfuerzos que la comunidad internacional aún debe desplegar para reducir la brecha digital.

La naturaleza evolutiva de las Tecnologías de la Información y Comunicaciones también se traduce en la creciente sofisticación de las amenazas en el ciberespacio, lo que exige una cooperación internacional más activa, principalmente en dos cuestiones que para mi delegación resultan fundamentales: garantizar, de conformidad con el derecho internacional vigente, el derecho de los Estados al acceso a las Tecnologías de la Información y Comunicación y a las tecnologías emergentes,

así como la transferencia de tecnologías de herramientas (software y hardware) destinadas al mantenimiento de un ciberespacio seguro y resiliente. Atento al carácter interoperable del ciberespacio, mi delegación sostiene la premisa de que ningún Estado podrá estar seguro hasta que todos estemos seguros.

Por último, la Argentina reafirma su compromiso de trabajar en colaboración con todos los Estados miembros y actores relevantes para abordar las amenazas cibernéticas de manera eficiente. Para ello, resulta fundamental promover la cooperación internacional para crear y fortalecer las capacidades de detección y respuesta ante incidentes cibernéticos a nivel global. También resulta de especial relevancia las medidas de fomento de la confianza en el ciberespacio y promover discusiones abiertas e inclusivas sobre las nuevas amenazas.

Muchas gracias!

Brazil

Mr. President,

Brazil shares the concern with the evolving cybersecurity threat landscape and we are in full agreement on the need for multilateral discussions to better identify common threats and find common solutions that can improve cyber resilience for all. However, in order to identify these commonalities, our discussions must be inclusive and they must not duplicate existing work.

As we have said in a similar Arria event last year, we believe the best forum for these discussions is the General Assembly. While we appreciate the ROK's convenening of an Arria formula meeting in order to broaden the discussion beyond the 15 members of the UNSC, any Arria formula meeting will necessarily still be more limited than a GA discussion with the full UN membership.

Mr. President,

The ongoing OEWG on security of ICTs has laid an important groundwork in the identification of cyber threats, which has highlighted both ransomware and cryptocrrency threats as well as other vectors of attack, including upon critical infrastructure. It has debated the spillover effects of cyber attacks and discussed how to guard and differentiate systems that are of particular humanitarian importance, with valuable insights from the ICRC. It has further clarified the the applicability of international law and international humanitarian law to cyberspace and is currently discussing the implementation of the framework for responsible state behavior in cyberspace. It will hold a Global Roundtable on capacity building next month and is already considering a mechanism for Regular Institutional Dialogue so as to ensure that our discussions and actions can continue to respond to evolving threats.

These are significant achievements, which illustrate the viability and the importance of holding these debates in a broad multilateral format in the appropriate forum. We are convinced that there are no shortcuts that beat broad-based dialogue towards shared understandings regarding cyber threats and how to counter them. The pace of developments in the cyber domain require a bold and prompt response to the challeges they may pose. However, we believe that the appropriate and legitimate forum to hold discussions and deliberations is the OEWG on security of ICTs.

I thank you.